EXHIBIT A

JEDI Cloud RFP

Solicitation Number: HQ003418R0077_JEDI_CLOUD_RFP

Agency: Other Defense Agencies
Office: Washington Headquarters Services
Location: WHS, Acquisition Directorate

Notice Type:
Combined Synopsis/Solicitation

Posted Date:
July 26, 2018

Response Date:
Sep 17, 2018 10:00 am Eastern

Archiving Policy:
Manual Archive

Archive Date:
-

Original Set Aside:
N/A

Set Aside:
N/A

Classification Code:
R – Professional, administrative, and management support services

NAICS Code:
518 – Data Processing, Hosting and Related Services/518210 – Data Processing, Hosting, and Related Services

Synopsis:
Added: Jul 26, 2018 9:00 am

Enclosed with this posting is a combined synopsis/solicitation for Joint Enterprise Defense Infrastructure (JEDI) Cloud for the Department of Defense. This announcement constitutes the formal Request for Proposal (RFP) and is prepared in accordance with the format provided in Federal Acquisition Regulation (FAR) Subpart 12.6, "Streamlined Procedures for Evaluation and Solicitation for Commercial Items," and supplemented with additional information in this notice.

We are excited by the level of interest in JEDI Cloud and appreciate industry's participation throughout the draft solicitation process. We are confident that these inputs helped us to refine and clarify the DoD's requirement represented in this RFP. We encourage you to read the letters from the DoD CIO and the Cloud Computing Program Manager provided as part of this RFP package to gain more insight into the requirement.

See RFP attachments for details, including deadlines for submission of proposals and instructions regarding In-Person Question and Answer Sessions.

Since the last release of comment/question responses, the Department received an additional 401 comments/questions from 16 Vendors and 1 Coalition in response to the second draft solicitation. We will not be sharing the identity of any commenters beyond these statistics. DoD remains committed to a transparent process. To that end, we are providing answers to these comments/questions along with this RFP.

In addition to the In-Person Question and Answer Sessions, questions or comments pertaining to this JEDI Cloud RFP shall be submitted via the attached Comment Resolution Matrix, which includes detailed instructions and format for submission. All feedback using the Comment Resolution Matrix must be emailed to jedi-rfp@dds.mil no later than August 16, 2018 at 11:00 am ET. Questions shall not contain any proprietary information since this information may not be publicly answered or published. Questions received after 11:00 am ET on August 16, 2018 may not be considered. Questions sent to any other email address will not be considered.

A list of documents being released with the JEDI Cloud RFP is included below for reference.

Related RFP Documents:
Comment Resolution Matrix
In-Person Q&A Session Information

RFP Attachments:
J-1 through J-5 to be provided by Offerors
J-6: JEDI Cloud Cyber Security Plan
J-7: DD Form 254, DoD Contract Security Classification Specification for ID/IQ
J-8: Definitions
J-9: Contract Data Requirements Lists (CDRLs) - Items A001 - A016
J-10: Small Business Participation Commitment Document

L-1: JEDI Cloud SOO
L-2: Price Scenarios
L-3: TO 001 PWS
L-4: TO 002 PWS
L-5: Price Scenario Price Build-Up Template
L-6: Small Business Subcontracting Plan Template
L-7: OCI Analysis/Disclosure Form
L-8: PWS/SOO & Factor Crosswalk Matrix
L-9: Non-disclosure Agreement for the Acquisition of the JEDI Cloud

Reference Documents:
Final Cloud Combined Congressional Report
DoD CIO RFP Release Letter
Program Manager RFP Release Letter
JEDI Cloud Industry and Government Q&A for draft RFP2
JEDI Cloud Single Award Determination and Findings
MIL-STD-810G CN1
CNSSP15

Thank you for your participation in this process.

JEDI Cloud RFP

Type: Other (Draft RFPs/RFIs, Responses to Questions, etc..)
Posted Date: July 26, 2018

Attachment_J-6_JEDI_Cyber_Security_Plan.pdf (2,299.61 Kb)
Description: Attachment J-6 : JEDI Cloud Cyber Security Plan

EXHIBIT B

DEPARTMENT OF DEFENSE
DEFENSE PENTAGON
WASHINGTON, D.C. 20301

July 26, 2018

Dear Industry Cloud Partners:

The Department of Defense (DoD) Joint Enterprise Defense Infrastructure (JEDI) Cloud Program takes great pleasure in releasing its final Request for Proposal (RFP) to industry. The intent of this release is to officially solicit proposals for the JEDI Cloud requirement. This final RFP captures the totality of the JEDI Cloud requirement. You will not need to refer to the earlier drafts to understand the Government's established position and/or requirement.

We received over 1,500 questions and comments in response to the multiple draft RFPs and have provided those questions, comments, and corresponding answers to industry, with the last round of questions, comments, and corresponding answers being released as part of this final RFP. There are a number of clarifications in this final release, including its attachments, that we want to bring to your attention.

- The option structure has been modified.
- The applicable requirements for Cross Domain Solutions have been clarified in the JEDI Cloud Cyber Security Plan.
- There are two security-related reference documents that are marked For Official Use Only (FOUO). There is a process provided in the final RFP for Offerors to execute a Non-Disclosure Agreement and receive these documents.
- The Price Scenarios have been further refined.
- The small business evaluation criteria have been further refined to allow for more flexibility while also striving to achieve DoD's small business objectives.
- The final RFP includes a new opportunity for In-Person Bidders' Question and Answer (Q&A) Sessions to augment the traditional written bidders Q&A process.

JEDI Cloud's security requirements are captured in the JEDI Cloud Cyber Security Plan, which includes an explanation of how other Federal government or DoD policies, such as National Industrial Security Program Operating Manual (NISPOM) and the DoD Cloud Computing Security Requirements Guide (CC SRG), apply to JEDI Cloud. There is no requirement for Offerors to have accredited classified environments at the time of proposal. The Statement of Objectives (SOO) requires the proposed solution to be available and meet the requirements as specified in the JEDI Cloud Cyber Security Plan within 30 days of contract award for unclassified services, within 180 days of contract award for classified services at the Secret level, and within 270 days of contract award for classified services at the Top Secret/Sensitive Compartmented Information (TS/SCI) and Special Access Program (SAP) levels. The awardee will submit its Security Authorization Package by each of these dates at which point DoD will process the package. The Gate Criteria for Sub-factor 1.2 - *'High*

Availability and Failover' specifies which services are required to have been certified at the time of proposal under the Federal Risk and Authorization Management Program (FedRAMP) requirements. The majority of certification requirements are for post award, which gives vendors time to meet the subset of requirements beyond what is already required for any vendor operating with the Federal Government.

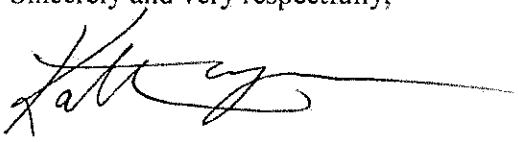
This production contract is key to allowing the Department to learn how to most effectively use cloud at the enterprise level. The JEDI Cloud will act as a pathfinder for us to understand how we can best achieve security, governance, and architectures at the enterprise level in a modern, relevant manner.

The Government will remain receptive to any comments/questions regarding this final RFP release that may serve to enhance your understanding and ultimately your ability to bid to the JEDI Cloud requirement. The Q&A period for the final RFP will close on August 16, 2018 at 11:00 AM ET.

In order to facilitate timely resolution and adjudication of your comments, questions, and/or concerns, it is imperative that you adhere to the response submission guidance and related format requirements provided in the Procuring Contracting Officer (PCO) instructions on FedBizOpps. Please understand that in order to maintain a fair and open process, only input received through the provided matrix and In-Person Q&A will be reviewed and considered.

This solicitation and associated contract award is open to any proposing team capable of meeting the Department's specified RFP requirements. Thank you for your attention to this letter and continued support of the JEDI Cloud acquisition.

Sincerely and very respectfully,



KAIGHT M. MEYERS, Lt Col, USAF
JEDI Cloud Computing Program Manager

EXHIBIT C

COMBINED SYNOPSIS/SOLICITATION FOR COMMERCIAL ITEMS

General Information RFP

Document Type:	Combined Synopsis/Solicitation (IAW FAR 12.603)
RFP Solicitation Number:	HQ0034-18-R-0077
Post Date:	July 26, 2018
Classification Code:	R -- Professional, Administrative, and Management Support Services
Set Aside:	Full and Open Competition
NAICS Code:	518210 – Data Processing, Hosting, and Related Services

Contracting Office Address

Washington Headquarters Services (WHS), Acquisition Directorate (AD)
4800 Mark Center Drive, Suite 09F09, Alexandria, VA 22350

Description

This is a combined synopsis/solicitation for commercial items prepared in accordance with the format in Federal Acquisition Regulation (FAR) Subpart 12.6, "Streamlined Procedures for Evaluation and Solicitation for Commercial Items," as supplemented with additional information included in this notice. This announcement constitutes the only solicitation. All non-price factors will be evaluated in accordance with (IAW) FAR Subpart 12.602 "Streamlined Evaluation of Offers". The price factor will be evaluated IAW FAR Subpart 12.209.

This solicitation is a Request for Proposal (RFP) for Joint Enterprise Defense Infrastructure (JEDI) Cloud for the Department of Defense (DoD). This RFP document and incorporated provisions and clauses are those in effect through Federal Acquisition Circular 2005-97 (Effective: 24 January 2018; updated with Class Deviation 2018-o0007) and DFARS Publication Notice 20180504 (Effective 04 May 2018). There is no assigned Defense Priorities and Allocations System (DPAS) rating for this requirement.

The associated North American Industrial Classification System (NAICS) code for this procurement is 518210 – "Data Processing, Hosting, and Related Services", with a small business size standard of $32.5M.

SECTION B: SUPPLIES OR SERVICES AND PRICES

Section B1: Schedule of Services – ID/IQ CLIN Structure

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001		As Ordered	Each	Priced by Catalog	

Unclassified IaaS and PaaS
FFP
Unclassified Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) offerings.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002		As Ordered	Each	Priced by Catalog	

Classified IaaS and PaaS
FFP
Classified IaaS and PaaS offerings

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003		As Ordered	Each	Priced by Catalog	

Unclassified Cloud Support Package
FFP
Unclassified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004		As Ordered	Each	Priced by Catalog	

Classified Cloud Support Package
FFP
Classified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005		As Ordered	Each	To Be Completed by Offeror	

Portability Plan
FFP
Deliver plan in accordance with CDRL A007.
Only the Cloud Computing Program Office (CCPO) has authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0006		As Ordered	Each	To Be Completed by Offeror	

Portability Test
FFP
Demonstrate portability of data and applications to other hosting environments. Only the CCPO has authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0007		24	Each	To Be Completed by Offeror	To Be Completed by Offeror

CCPO PM Support
FFP
CCPO Program Management (PM) CLIN will be performed per Section C2. Only the CCPO has authority to order under this CLIN. For the purpose of this CLIN, the unit of issue “EACH” equates to a month of services.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001		As Ordered	Each	Priced by Catalog	
OPTION	Unclassified IaaS and PaaS FFP Unclassified IaaS and PaaS offerings				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002		As Ordered	Each	Priced by Catalog	
OPTION	Classified IaaS and PaaS FFP Classified IaaS and PaaS offerings				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1003		As Ordered	Each	Priced by Catalog	
OPTION	Unclassified Cloud Support Package FFP Unclassified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1004		As Ordered	Each	Priced by Catalog	
OPTION	Classified Cloud Support Package FFP Classified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1005		As Ordered	Each	To Be Completed by Offeror	

OPTION Portability Plan
FFP
Deliver plan in accordance with CDRL A007.
Only the CCPO has the authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1006		As Ordered	Each	To Be Completed by Offeror	

OPTION Portability Test
FFP
Demonstrate portability of data and applications to other hosting environments. Only the CCPO has the authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1007		36	Each	To Be Completed by Offeror	To Be Completed by Offeror

OPTION CCPO PM Support
FFP
CLIN will be performed IAW Section C2.
Only the CCPO has the authority to order under this CLIN. For the purpose of this CLIN, the unit of issue “EACH” equates to a month of services.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001		As Ordered	Each	Priced by Catalog	
OPTION	Unclassified IaaS and PaaS FFP Unclassified IaaS and PaaS offerings				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002		As Ordered	Each	Priced by Catalog	
OPTION	Classified IaaS and PaaS FFP Classified IaaS and PaaS offerings				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2003		As Ordered	Each	Priced by Catalog	
OPTION	Unclassified Cloud Support Package FFP Unclassified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2004		As Ordered	Each	Priced by Catalog	
OPTION	Classified Cloud Support Package FFP Classified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2005		As Ordered	Each	To be Completed by Offeror	

OPTION Portability Plan
FFP
Deliver plan in accordance with CDRL A007.
Only the CCPO has the authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2006		As Ordered	Each	To be Completed by Offeror	

OPTION Portability Test
FFP
Demonstrate portability of data and applications to other hosting environments. Only the CCPO has the authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2007		36	Each	To Be Completed by Offeror	To Be Completed by Offeror

OPTION CCPO PM Support
FFP
CLIN will be performed IAW Section C2
Only the CCPO has the authority to order under this CLIN. For the purposes of this CLIN, the unit of issue “EACH” equates to a month of services.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001		As Ordered	Each	Priced by Catalog	
OPTION	Unclassified IaaS and PaaS FFP Unclassified IaaS and PaaS offerings				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002		As Ordered	Each	Priced by Catalog	
OPTION	Classified IaaS and PaaS FFP Classified IaaS and PaaS offerings				

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3003		As Ordered	Each	Priced by Catalog	

OPTION Unclassified Cloud Support Package
FFP
Unclassified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3004		As Ordered	Each	Priced by Catalog	

OPTION Classified Cloud Support Package
FFP
Classified offerings of catalog support to advise and assist with architecture, usage, provisioning, and configuration of IaaS and PaaS, to include homefront to the tactical edge. Package services may advise and assist with integration, aggregation, orchestration, and troubleshooting of cloud services. Package may include training services, materials, and documentation for available services. This is not a time-and-materials or labor-hour based CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3005		As Ordered	Each	To be Completed by Offeror	

OPTION Portability Plan
FFP
Deliver plan in accordance with CDRL A007.
Only the CCPO has the authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3006		As Ordered	Each	To be Completed by Offeror	

OPTION Portability Test
FFP
Demonstrate portability of data and applications to other hosting environments. Only the CCPO has the authority to order under this CLIN.

NET AMT

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3007		24	Each	To Be Completed by Offeror	To Be Completed by Offeror

OPTION CCPO PM Support
FFP
CLIN will be performed IAW Section C2
Only the CCPO has the authority to order under this CLIN. For the purposes of this CLIN, the unit of issue “EACH” equates to a month of services.

NET AMT

Section B2: Maximum Contract Limit and Minimum Contract Guarantee

1. The successful awardee's fixed unit price information (CLIN x005 Portability Plan, x006 Portability Test, and x007 CCPO PM Support) and proposed catalog offerings will be incorporated into the resultant Indefinite-Delivery, Indefinite-Quantity (ID/IQ) contract and will serve as the basis for establishing overall task order (TO) pricing for the duration of the ID/IQ.

2. Maximum. The maximum, as that term is used in FAR clause 52.216-22, is $10,000,000,000.00. Hence, the cumulative amount of all TOs issued under this contract shall not exceed $10,000,000,000.00.

3. Minimum. The minimum guaranteed award amount for the JEDI Cloud ID/IQ Contract is $1,000,000.00. The exercise of any option does not re-establish the contract minimum guarantee.

4. The Government has no obligation to issue TOs under the resultant ID/IQ contract beyond the amount specified in paragraph three.

Section B3: Task Order Contract Types

This single award ID/IQ contract allows for the placement of TOs by DoD warranted Contracting Officers. All TOs will be firm-fixed price.

Section B4: Travel

Travel is not anticipated. However, if the JEDI Cloud Contracting Officer later determines that travel is necessary for TO performance under this ID/IQ, the contract will be modified accordingly.

Section B5: Security

All tasks in support of JEDI Cloud must be conducted IAW Attachment J-6, JEDI Cloud Cyber Security Plan; Attachment J-7, DD Form 254, DoD Contract Security Classification Specification for ID/IQ; and other security requirements in the contract. Future TO DD Form 254s are anticipated to be identical to Attachment J-7 with the exception of Block 16, Certification and Signature, and Block 17, Required Distribution. Each TO ordering activity will complete Blocks 16 and 17 as appropriate.

SECTION C: DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

Section C1: Performance Work Statement

ID/IQ: The Offeror's Performance Work Statement (PWS), proposed in response to the Government's Attachment L-1 JEDI Cloud Statement of Objectives (SOO), will be incorporated into the contract as Attachment J-2. The Offeror shall meet all requirements of Attachment J-6, JEDI Cloud Cyber Security Plan. In the event of a conflict between the JEDI Cloud Cyber Security Plan and the PWS, the JEDI Cloud Cyber Security Plan takes precedence over the PWS. For administration purposes both the PWS and the JEDI Cloud Cyber Security Plan are listed as attachments in Section J. However, for the purpose of FAR 52.212-4(s), they shall be deemed incorporated into Section C1.

All Performance Metrics listed in the PWS shall apply to all TOs unless otherwise noted. Migration services are outside the scope of this contract.

Section C2: Program Management

1. The Contractor shall provide overarching program management personnel, processes, and tools under CLINs x007 necessary to manage and oversee all contract activities for the duration of the ID/IQ within schedule, quality, and performance requirements. The Contractor shall establish and maintain a formal program management organization, which shall coordinate and interface with the CCPO. The Contractor shall appoint a Program Manager (PM) and Deputy PM empowered to make program and project level decisions and commit resources necessary to successfully execute courses of action within scope of this contract. Two key functions of the Contractor's program management support will be facilitating the timely authentication and authorization of JEDI Cloud infrastructure and offerings at all classification levels and coordinating successful integration of the DoD's provisioning tool. The PM and Deputy PM shall have sufficient expertise and authority to execute the following responsibilities as the authorized official: (a) serve as the official central point of contact and interface between the Contractor and the CCPO PM, (b) be available as needed for CCPO interaction, and (c) monitor and report on contract status (CDRL A001), Service Level Agreements (SLAs), and compliance with all contract requirements.

2. The Government will use the Quality Assurance Plan (QASP) as one mechanism to oversee Contractor performance. A majority of TOs are unlikely to have TO-level QASPs; however, the Government retains the right to implement QASPs at the TO level. The Contractor's Quality Control Plan (QCP) (CDRL A010) will establish methodologies by which the Contractor will meet or exceed schedule, quality, and performance requirements.

3. The Contractor shall implement a Small Business Participation Commitment Document (Attachment J-10). This will assist in the development of capabilities of small businesses and provide a maximum practicable opportunity to participate in efficient contract performance for small businesses. The Contractor shall report on small business participation in the Small Business Reporting (CDRL A013).

Section C3: Transition Out

1. **Transition Out Plan:** When requested by the JEDI Cloud Contracting Officer, the Contractor will have up to 60 days to provide a Transition Out Plan (CDRL A002). The purpose of the Transition Out Plan is to explain to the CCPO the procedures necessary to transition either all or a part of the services under this contract, as directed by the Government. The Transition Out Plan shall describe detailed recommendations for maintaining continuity of services and preventing degradation of services during the transition period. The Transition Out Plan shall provide recommendations on how account holders may efficiently extract their application(s) and user data in a manner that is consistent with the Portability Plan. The Transition Out Plan shall address the unclassified environment, classified environment, and tactical edge offerings separately. Further, the Contractor shall explain the process to provide knowledge transfer to the CCPO and include job shadowing for up to 30 days, training, and other activities in order to successfully transition the environment to the new hosting environment. The Transition Out Plan shall include a process for identifying and destroying all classified infrastructure, materials, or information IAW CCPO instructions and the contract's security requirements.

2. **Transition Out Execution:** The Contractor shall perform all activities as described in the approved Transition Out Plan, excluding extraction of applications and data, which is a user responsibility. The Contractor shall exercise its best efforts and cooperation to effect an orderly and efficient transition to a successor. The Contractor shall deliver all technical data, computer software, and computer software documentation generated in the performance of this contract, to which the Government has rights. The Contractor shall execute knowledge transfer in accordance with the Transition Out Plan. When directed, the Contractor shall purge all unclassified materials and information and purge or destroy, as appropriate, all classified infrastructure, materials, and information IAW the Transition Out Plan. The Contractor shall return any Government Furnished

Property (GFP) or Government Furnished Information.

Section C4: Contractor Control of Certain Parts of JEDI Cloud

1. The legally enforceable ability for the prime contractor to maintain control over certain parts of JEDI Cloud is critical to meeting the security requirements of this contract. The Government expects that it will need to direct the Contractor to affect alterations or configuration changes to JEDI Cloud for purposes of addressing critical security vulnerabilities. The Contractor must be able to decisively and rapidly respond in the interests of national defense. For the purpose of this section, the direction concerning critical security vulnerabilities may come from the DoD CIO in coordination with the JEDI Cloud Contracting Officer and CCPO PM.

2. For purpose of this section, "rapidly" means in 8 hours or less from Government notification. All Government-directed alterations or configurations changes will be agreed upon by both the Government and the Contractor prior to implementation.

3. Depending on the urgency of the circumstances, the agreed-to alteration or configuration change may initially be achieved by oral direction from the JEDI Cloud Contracting Officer, but to the extent it is deemed a "change" as defined by FAR clause 52.212-4(c), the change will be subsequently reflected in a written agreement of the parties as soon as practicable.

4. Throughout the entire period of performance, the Contractor shall maintain control, as defined in this section, over the following parts of JEDI Cloud for both the unclassified and classified environments:

   a. Underlying hardware infrastructure, including networking components within the data centers;
   b. Underlying software layer, including the hypervisor and networking components;
   c. Software platform offerings (excluding third-party marketplace offerings); and
   d. Hardware and software components of all points of presence.

5. "Control" means that, for the part of JEDI Cloud in paragraph 1 above, the prime contractor either:

   a. Is the owner, as defined in this section, paragraph 6, as evidenced by self-certification. The Government may request additional documentation to prove ownership at any time and with any frequency throughout the period of performance; or
   b. Has a bilaterally signed agreement (Control Agreement) that is binding for at least 11 years with the owner granting the prime contractor the following rights:
      i. Unrestricted physical access; and
      ii. An ability to rapidly affect changes to the owned parts.

      This Control Agreement must state that it may not be terminated by the Owner without at least 120 days notice to the Government. The JEDI Cloud Contracting Officer may request confirmation that the Control Agreement has not been altered or terminated at any time.

6. "Owner" means that, for the parts listed in paragraph 1, the entity has a legally enforceable claim or title, which includes the rights listed in sub-paragraphs 5.b.i and 5.b.ii. The owner must have a legally binding and recorded document evidencing ownership.

SECTION D: PACKAGING AND MARKING

Packaging and Marking Requirements will be delineated in individual TOs.

SECTION E: INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
0002	Destination	Government	Destination	Government
0003	Destination	Government	Destination	Government
0004	Destination	Government	Destination	Government
0005	Destination	Government	Destination	Government
0006	Destination	Government	Destination	Government
0007	Destination	Government	Destination	Government
1001	Destination	Government	Destination	Government
1002	Destination	Government	Destination	Government
1003	Destination	Government	Destination	Government
1004	Destination	Government	Destination	Government
1005	Destination	Government	Destination	Government
1006	Destination	Government	Destination	Government
1007	Destination	Government	Destination	Government
2001	Destination	Government	Destination	Government
2002	Destination	Government	Destination	Government
2003	Destination	Government	Destination	Government

2004	Destination	Government	Destination	Government
2005	Destination	Government	Destination	Government
2006	Destination	Government	Destination	Government
2007	Destination	Government	Destination	Government
3001	Destination	Government	Destination	Government
3002	Destination	Government	Destination	Government
3003	Destination	Government	Destination	Government
3004	Destination	Government	Destination	Government
3005	Destination	Government	Destination	Government
3006	Destination	Government	Destination	Government
3007	Destination	Government	Destination	Government

SECTION F: PERFORMANCE

Section F1: Contract Period of Performance / Ordering Periods

The Period of Performance (PoP) of the resulting ID/IQ contract is structured as one continuous two-year base ordering period, two continuous three-year option ordering periods, and one continuous two-year option ordering period for a potential total of 10 years. After the ID/IQ Ordering PoP expires, the ID/IQ terms and conditions remain effective until performance under the final TO is completed and shall govern the active TOs to the same extent as if their periods of performance were active during the requisite ID/IQ ordering period.

The ordering period structure for the resulting ID/IQ contract is detailed below (with anticipated timeframes):

Base Ordering Period (2 years)	April 17, 2019 - April 16, 2021
Option Ordering Period 1 (3 years)	April 17, 2021 - April 16, 2024
Option Ordering Period 2 (3 years)	April 17, 2024 - April 16, 2027
Option Ordering Period 3 (2 years)	April 17, 2027 - April 16, 2029

Section F2: Task Order Period of Performance

1. Under no circumstances may a new TO be placed under the ID/IQ if the contract is terminated or has expired; and

2. From the date the TO is placed, the PoP, inclusive of options, may only exceed one year beyond the applicable PoP of the ID/IQ.

Section F3: Place of Performance

The services to be provided under the ID/IQ contract shall be accomplished at the locations identified in the TOs and may necessitate effort in the Contiguous United States (CONUS) and Outside the CONUS (OCONUS).

Section F4: Contractor Performance Evaluation

Interim and final evaluations of the Contractor performance will be prepared on the ID/IQ contract and on each resulting TO IAW FAR Subpart 42.15 and DoD Class Deviation 2013-O0018 that has a total value above $1,000,0000. The final performance evaluation will be prepared at the time of contract completion. In addition to the final evaluation, interim evaluation(s) will be prepared annually and prior to exercising an option.

Interim and final evaluations will be provided to the Contractor as soon as practicable after completion of the evaluation. The Contractor will be permitted 30 days to review the document and either submit additional information or a rebutting statement. If agreement cannot be reached between the parties, the matter will be referred to an individual one level above the Contracting Officer, whose decision will be final.

Copies of the evaluations, Contractor responses, and review comments, if any, will be retained as part of the contract file, and may be used to support future award decisions.

Contractors may access evaluations through a secure Web site for review and comment at the following address:

https://www.cpars.gov

Section F5: Government Furnished Property

The following GFP will be issued under this contract:

1. Type 1 Cryptography Devices
2. Encryption Hardware

Section F6: Organizational Conflict of Interest (OCI)

During the period of performance, the Contractor shall notify the Government if any potential or actual OCI, as described in FAR Subpart 9.5, exists for this contract for itself or its subcontractors. If the Contractor believes that an actual or perceived OCI does exist on this contract, the Contractor shall submit an OCI Mitigation Plan, explaining in detail how the OCI will be mitigated and/or avoided.

Section F7: Method of Ordering

All DoD Contracting Offices and Ordering Activities are authorized to place TOs under the JEDI Cloud ID/IQ contract IAW their delegated contracting authority. Ordering Contracting Officers (OCOs) may issue TOs for services subject to their respective contracting warrant limitations. OCOs have no authority to modify, add, or delete any terms and/or conditions in the base ID/IQ contract. JEDI Cloud ID/IQ contract terms and conditions supersede TO special instructions, terms and/or conditions where they may otherwise conflict.

Section F8: Task Order Performance

At a minimum, the following paragraphs shall be applicable to all TOs issued under this contract, unless otherwise specified in an individual TO.

1. The Contractor shall, IAW the terms and conditions set forth hereafter, execute all activities necessary and incidental to the completion of the contractual effort.

2. When the Contractor encounters difficulty in meeting performance requirements, or anticipates difficulty in complying with the contract delivery schedule or date, it shall immediately notify the OCO and JEDI Cloud Contracting Officer in writing giving pertinent details; provided, however, that this data shall be informational only in character and that this provision shall not be construed as a waiver by the Government of any delivery schedule or any rights or remedies provided by law or under this contract.

Section F9: Task Order Administration

1. Each Ordering Activity is responsible for administration of its own TOs. JEDI Cloud ID/IQ contract terms and conditions supersede TO special instructions, terms, and/or conditions where they may otherwise conflict. Requests for deviations or modification of the basic contract must be submitted to the JEDI Cloud Contracting Officer. Terminations of TOs shall be issued by the Ordering Activity. The CCPO PM shall be notified of any terminations.

2. A Contracting Officer Representative shall be appointed for each TO IAW the instruction of the Ordering Activity.

Section F10: Task Order Procedures

Specific instructions on how to place TOs against this ID/IQ will be provided in the ordering guide (CDRL A008).

Section F11: Clause(s)

The following clause(s) are included by reference:

52.242-17	Government Delay Of Work	APR 1984

SECTION G: CONTRACT ADMINISTRATION DATA

Section G1: Clauses Incorporated By Full Text

252.201-9000 WHS/AD LOCAL CLAUSE: CONTRACTING OFFICER'S REPRESENTATIVE (COR) (MAR 2015)

(a) The Contracting Officer's Representative (COR) is a representative of the Government with limited authority who has been designated in writing by the Contracting Officer to provide technical direction, clarification, and guidance with respect to existing specifications and performance work statement/statement of work/statement of objectives, as established in the contract. The COR also monitors the progress and quality of the Contractor's performance for payment purposes. The COR shall promptly report Contractor performance discrepancies and suggested corrective actions to the Contracting Officer for resolution.

(b) The COR is not authorized to take any direct or indirect actions or make any commitments that will result in changes to price, quantity, quality, schedule, place of performance, delivery or any other terms or conditions of the written contract.

(c) The Contractor is responsible for promptly providing written notification to the Contracting Officer if it believes the COR has requested or directed any change to the existing contract. No action shall be taken by the Contractor for any proposed change to the existing contract. No action shall be taken by the Contractor for any proposed change to the contract until the Contracting Officer has issued a written directive or a written modification to the contract. The Government will not accept and is not liable for any alleged change to the contract unless the change is included in a written contract modification or directive signed by the Contracting Officer.

(d) COR authority is not delegable.

(e) The COR for this contract is: Specified at time of award in the COR Designation Memorandum.

(end of clause)

252.204-7006 BILLING INSTRUCTIONS (OCT 2005)

When submitting a request for payment, the Contractor shall—
(a) Identify the contract line item(s) on the payment request that reasonably reflect contract work performance; and
(b) Separately identify a payment amount for each contract line item included in the payment request.

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

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

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the System for Award Management at https://www.acquisition.gov; and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this Web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the “Web Based Training” link on the WAWF home page at https://wawf.eb.mil/.

(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).

2n1 Services

(Contracting Officer: Insert applicable document type(s). Note: If a “Combo” document type is identified but not supportable by the Contractor's business systems, an “Invoice” (stand-alone) and “Receiving Report” (stand-alone) document type may be used instead.)

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

Inspect/Accept: TDB

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table to be populated for individual TOs

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	
Issue By DoDAAC	
Admin DoDAAC	
Inspect By DoDAAC	
Ship To Code	
Ship From Code	
Mark For Code	
Service Approver (DoDAAC)	
Service Acceptor (DoDAAC)	

Accept at Other DoDAAC
LPO DoDAAC
DCAA Auditor DoDAAC
Other DoDAAC(s)
---

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the email address identified below in the "Send Additional Email Notifications" field of WAWF once a document is submitted in the system.

TDB

(g) WAWF point of contact. (1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

TBD

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

(End of clause)

SECTION H: SPECIAL CONTRACT REQUIREMENTS

The Contractor shall flowdown any Section H clauses that specifically require flowdown notwithstanding the language in (b)(1) of 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (DEVIATION 2013-O0019) (SEP 2013).

Section H1: Government Data

1. The Government reserves all rights, title and interest (including all intellectual property and proprietary rights) in and to: a) any computer software (including machine images and databases) or data (including text, audio, video, and images) that the Government transfers to, develops in, or generates in JEDI Cloud for processing, storage, or hosting; b) any computational results or data derived from the use of JEDI Cloud services; and c) any JEDI Cloud account information.

2. The Contractor may not prevent or otherwise impede JEDI Cloud users from exporting any items under paragraph 1, and/or any associated databases, object and file storage, system configurations, cloud activity logs, and network configurations. Within 30 days of expiration of the contract, the Contractor shall destroy any items under paragraph 1 that remain hosted in JEDI Cloud or are in the possession or control of the Contractor.

3. Any service usage data associated with JEDI Cloud users may be used for purposes of providing or improving services under the contract. Such service usage data may not be sold to third parties. Under no circumstances may the Contractor disclose JEDI Cloud account information to third

parties unless those third parties are approved subcontractors under the contract and such disclosure is necessary for contract performance.

4. Before reusing unclassified infrastructure for another non-DoD tenant, the Contractor may be required to purge the storage media IAW Attachment J-6, JEDI Cloud Cyber Security Plan and any specific instructions included in a TO. The Contractor must request and obtain CCPO approval prior to conducting any unclassified infrastructure and/or media destruction IAW Attachment J-6, JEDI Cloud Cyber Security Plan and any specific instructions included in a TO.

5. The Contractor is prohibited from reusing classified infrastructure for another non-JEDI user tenant or at a different classification level from which the infrastructure has been accredited without CCPO approval; the Contractor is prohibited from transferring any classified infrastructure to a non-JEDI user. The Contractor may be required to purge classified storage media and/or destroy classified infrastructure IAW Attachment J-6, JEDI Cloud Cyber Security Plan and any specific instructions included in a TO. The Contractor must request and obtain CCPO approval prior to conducting any classified storage media purging, classified storage media destruction, or classified infrastructure destruction IAW Attachment J-6, JEDI Cloud Cyber Security Plan and any specific instructions included in a TO.

Section H2: New Services

1. When new (including improved) IaaS, PaaS, or Cloud Support Package services are made publicly available to the commercial marketplace in the continental United States (CONUS) and those services are not already listed in the JEDI Cloud catalogs in Attachment J-1: Price Catalogs, the Contractor must immediately (no later than 5 calendar days) notify the JEDI Cloud Contracting Officer for incorporation of the new services into the contract in accordance with the Performance Work Statement. At its discretion, the Contractor may also seek to incorporate new services into the contract in advance of availability to the commercial marketplace. The JEDI Cloud Contracting Officer must approve incorporation of any new services into the contract.

2. Any discounts, premiums, or fees in Attachment J-3: Contractor Discounts, Premiums, and Fees shall equally apply to new services, unless specifically negotiated otherwise.

3. The price incorporated into the JEDI Cloud catalog for new unclassified services shall not be higher than the price that is publicly-available in the commercial marketplace in CONUS, plus any applicable discounts, premiums or fees pursuant to paragraph 2.

   a. New services that are proposed to be incorporated into the contract in advance of availability to the commercial marketplace may potentially be considered a noncommercial item. The JEDI Cloud Contracting Officer will make a fact specific commerciality determination. If the new service is not a commercial item and no other exception or waiver applies, the JEDI Cloud Contracting Officer may require certified cost and pricing data or other than certified cost and pricing data under FAR Subpart 15.4 to make a fair and reasonable price determination.

      i. If there are any new fees associated with a new service that is proposed to be incorporated into the contract in advance of availability to the commercial marketplace, the new proposed fee must be provided to the JEDI Cloud Contracting Officer for review and, if appropriate, approval and incorporation into the contract.

4. The price incorporated into the JEDI Cloud catalog for new classified services may include a price premium as compared to unclassified services because of the additional security requirements.
   a. The allowable classified price premium for new services for the entire remaining

period of performance is the lesser expensive premium among the following:

i. The price premium applicable to the most comparable classified service, as compared to the price for the comparable unclassified service, at the time of contract award; or

ii. The following classified price premium as completed by the contractor as part of its proposal: *to be completed by Offeror*; or

iii. The price premium proposed by the Contractor at the time the new service is made available to the Government.

5. If a service that is ordered pursuant to a TO in the Attachment J-1, Price Catalogs is eliminated from the Contractor's publicly-available commercial catalog, the Contractor shall offer the Government replacement service(s) with substantially similar functionality as, and at a price no higher than, the service being eliminated for the entire remaining PoP of the applicable TO(s). The replacement service(s) shall be made available at least 30 days before the service is suspended. Under no circumstances may the replacement service(s) require purchase of additional services that causes the price to be higher than the eliminated service in order to achieve the same functionality of the eliminated service.

6. When the JEDI Cloud Contracting Officer incorporates the new service into the Attachment J-1, Price Catalogs and/or Attachment J-3: Contractor Discounts, Premiums, and Fees, the Contractor shall update the listing of services and corresponding prices in the online pricing calculator and application programming interfaces (APIs) for JEDI Cloud within 24 hours.

Section H3: Price Changes

1. Within 45 calendar days of the Contractor lowering prices in its publicly-available commercial catalog in CONUS, the Contractor shall submit a revised catalog for incorporation into Attachment J-1, Price Catalogs as follows:

a. For unclassified services, the revised catalog price shall match the commercially lower price.

b. For classified services, the revised catalog price shall be lowered by *to be completed by Offeror* percentage of the net value difference for the newly lowered rate for the unclassified service.

i. For example, if an unclassified service is lowered from $1.00 to $0.75, resulting in a net value difference of $0.25, and the percentage in paragraph (b) above is 100%, then the classified service would also be lowered by $0.25; however, if the percentage in paragraph (b) above is 50% then the classified service would be lowered by $0.125.

2. Any discounts, premiums, or fees in Attachment J-3: Contractor Discounts, Premiums, and Fees shall equally apply to any services with price changes, unless specifically negotiated otherwise.

3. The Contractor may offer new or additional discounts at any time to be incorporated into Attachment J-3: Contractor Discounts, Premiums, and Fees only upon JEDI Cloud Contracting Officer approval.

4. When the JEDI Cloud Contracting Officer incorporates the revised price into the Attachment J-1, Price Catalogs and/or Attachment J-3: Contractor Discounts, Premiums, and Fees, as appropriate, the Contractor shall update the listing of services and corresponding prices in the online pricing calculator and APIs for JEDI Cloud within 24 hours.

Section H4: Additional Security

1. Security requirements is one material condition of this contract. This contract and any resulting TOs shall be subject to immediate termination for cause, without the requirement for a cure notice, when it has been determined by the JEDI Cloud Contracting Officer that a failure to fully comply with the security requirements of this contract resulted from the willful misconduct or lack of good faith on the part of any one of the Contractor's directors or officers, or on the part of any of the managers, superintendents, or equivalent representatives of the Contractor who have supervision or direction of:

a. All or substantially all of the Contractor's Cloud business, or
b. All or substantially all of the Contractor's operations at any one plant or separate location in which this contract is being performed, or
c. A separate and complete major industrial operation in connection with the performance of this contract.

2. The legally enforceable ability for the prime contractor to maintain control over certain parts of JEDI Cloud is another material condition of this contract. This contract and any resulting TOs shall be subject to immediate termination for cause, without the requirement for a cure notice, when it has been determined by the JEDI Cloud Contracting Officer that a failure to fully comply with the security requirements of this contract resulted from the lack of control required by Section C4.

Section H5: Issuance of Subcontracts

1. The Contractor shall provide to the JEDI Cloud Contracting Officer written notice of all subcontracts issued under this contract. For the purpose of this requirement, subcontract means a contract, as defined in FAR Subpart 44.101.

2. The JEDI Cloud Contracting Officer's written consent is required for all subcontractors performing classified services under the contract.

Section H6: Limited Release Of Contractor Confidential Business Information

1. "Confidential Business Information," (Information) as used in this clause, is defined as all forms and types of financial, business, economic, or other types of information including technical data or computer software/computer software documentation, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing even when -- (a) the owner thereof has taken reasonable measures to keep such information secret, and (b) the Information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through, proper means by the public. Information will include technical data, as that term is defined in DFARS 252.227-7013(a)(14) and 252.227-7015(a)(4). Similarly, Information does include computer software/computer software documentation, as those terms are defined in DFARS 252.227-7014(a)(4).

2. The Government may release to individuals, employed by support contractors and their subcontractors, Information submitted by the Contractor or its subcontractors pursuant to the provisions of this contract. Information that would ordinarily be entitled to confidential treatment may be included in the Information released to these individuals. Accordingly, by submission of a proposal or execution of this contract, the Offeror or Contractor and its subcontractors consent to a

limited release of its Information, but only for purposes as described in paragraph (3) of this clause.

3. Circumstances where the Government may release the Contractor's or subcontractors' Information include the following:

a. To other contractors and subcontractors, and their employees tasked with assisting the Government in handling and processing Information and documents in the administration of contracts, such as file room management and contract closeout;
b. To other contractors and subcontractors, and their employees tasked with assisting the Government in accounting support services,
c. To other contractors and subcontractors, and their employees tasked with assisting the Government in technical and administrative support services for the JEDI Cloud program, including monitoring contract progress and providing financial oversight; and,
d. To other contractors and subcontractors, and their employees tasked with assisting the Government in furnishing advice or technical assistance in support of the Government's management and oversight of the JEDI Cloud program.

4. The Government recognizes its obligation to protect the Contractor and its subcontractors from competitive harm that could result from the release of such Information. The limited release of Information under paragraphs (3)(a-d) are permitted only under the following conditions:

a. The Government determines that access is required by other contractors and their subcontractors to perform the tasks described in paragraphs (3)(a-d);
b. Access to Information is restricted to individuals with a bona fide need to possess;
c. Contractors and their subcontractors having access to Information have agreed under their contract or a separate corporate non-disclosure agreement to provide the same level of protection to the Information that would be provided by Government employees. Such contract terms or separate corporate non-disclosure agreement shall require the contractors and subcontractors to train their employees on how to properly handle the Information to which they will have access, and to have their employees sign company non-disclosure agreements certifying that they understand the sensitive nature of the Information and that unauthorized use of the Information could expose their company to significant liability. Copies of such employee non-disclosure agreements shall be provided to the Government;
d. Contractors and their subcontractors performing the tasks described in paragraphs (3)(a-d) have agreed under their contract or a separate non-disclosure agreement to not use the Information for any purpose other than performing the tasks described in paragraphs (3)(a-d); and
e. Contractors and their subcontractors having access to technical data, computer software, or computer software documentation have executed the Use and Non-Disclosure Agreement specified at DFARS 227.7103-7 or have DFARS 252.227-7025 in their contract.

5. The Government's responsibilities under the Freedom of Information Act (FOIA) are not affected by this clause.

6. The Contractor is a third-party beneficiary to any non-disclosure agreement entered into by the recipient with the Government or any other non-contractor party.

Section H7: Non-Endorsement

This contract does not, in any manner, constitute an endorsement by the Government of any results, services, resulting designs, hardware, software or any other applications resulting from performance under this contract. This contract does not obligate the Government to award future contracts to Contractor.

Section H8: Mandatory Addendum License Agreement or Service Level Agreement

1. The following Addendum shall be used for any License Agreements (whether called an End User License Agreement, Terms of Use, or some other name) and Service Level Agreements (SLAs) . The list of terms in the Addendum is not necessarily all-inclusive, but is intended to convey and resolve the most common terms that are problematic to the Government. Problematic terms beyond those in the Addendum will have to be specifically negotiated prior to acceptance of the License Agreement or SLA.
2. The only License Agreements (whether called an End User License Agreement, Terms of Use, or some other name) and SLAs applicable to JEDI Cloud users are those agreements attached to the contract in Attachment J-5: Licenses and Service Level Agreements with the following exception:
    a. Revisions to agreements in Attachment J-5: Licenses and Service Level Agreements may immediately take effect if those revisions do not: i. conflict with a contract requirement in the Performance Work Statement, Cyber Security Plan, or contract terms and conditions; ii. materially affect the Government's obligations; iii. increase contract prices; iv. decrease the level of service; or v. otherwise limit any Government rights under the contract. The Contractor agrees that any revisions that violate this paragraph are not enforceable against the Government.

    b. The Contractor shall submit revised agreements under this exception to the JEDI Cloud Contracting Officer for review within 30 days of the revision.

3. The Contractor may submit new or revised License Agreements or SLAs after award for incorporation into the contract upon review and approval by the JEDI Cloud Contracting Officer. Such post-award License Agreements and SLAs will be reviewed for consistency with Federal law and the Government's needs, which are reflected in the requirements in Section C1: Performance Work Statement and the JEDI Cloud Cyber Security Plan and Section H1: Government Data.
3. The Government will accept commercial terms in a License Agreement or SLA only to the extent that those terms do not conflict with Federal law and only to the extent those terms meet the Government's needs.

4. The Contractor agrees that, in the event of any conflict or inconsistency between the terms in this Addendum and the terms of the License Agreement or SLA, the terms of this Addendum will supersede and be controlling. The Contractor acknowledges that this Addendum is a binding part of its contract and all TOs issued thereunder.

ADDENDUM TO LICENSE AGREEMENT

Addendum to License Agreement or Service Level Agreement

The Contractor, _____, hereby submits this Addendum as an attachment to the License Agreement, whether called an End User License Agreement, Terms of Use, or some other name or Service Level Agreements (SLAs). The Contractor agrees that, in the event of any conflict or inconsistency between the terms in this Addendum and the terms of the License Agreement or SLAs, the terms of this Addendum will supersede and be controlling.

The Government accepts commercial terms in a License Agreement or SLA only to the extent that those terms do not conflict with Federal law and only to the extent those terms meet the Government's needs. The Government's needs are the requirements in Section C1: Performance Work Statement attached to the contract and the JEDI Cloud Cyber Security Plan and Section H1: Government Data.

687
688 The following terms, when they appear in a License Agreement, have been determined unacceptable
689 to the Government as a result of a conflict with Federal law or as a result of incompatibility with the
690 Government's needs. Any such terms in a License Agreement or SLA will have no force or effect in
691 any resulting contract.
692

General Indemnity (by the government)	The Government does not agree to indemnify any party because such agreements may violate the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1)(B). Instead, recourse against the United States for any alleged breach of this agreement must be as a dispute under the contract disputes clause (Contract Disputes Act). While a dispute is pending, the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer.
Patent Indemnity (by the Contractor)	Clauses giving the Contractor control over any claims or disputes involving patent or other intellectual property infringement are not allowable, insofar as only the US Department of Justice is authorized to represent the US Government, per 28 U.S.C. § 516. Any clause giving entire control of litigation to a Contractor is hereby modified as follows: If a third party claims that products or services delivered under this contract infringe that party's patent or copyright, the Contractor will indemnify the Government against liability, at the Contractor's expense, and pay all costs, damages, and attorney's fees that a court finally awards or that are included in a settlement approved by the Contractor, provided that the Government promptly notifies the Contractor of the claim and gives the Contractor such opportunity as is offered by applicable laws, rules, and regulations to participate in the defense thereof. The Government shall make every effort to fully participate in the defense and/or in any settlement of such claim. However, the Contractor understands that such participation will be under the control of the U.S. Department of Justice, per 28 U.S.C. § 516.

Automatic renewals (e.g., term licenses for software or software maintenance that renew automatically and renewal charges are due automatically unless the government takes action to opt out or terminate)	The Government does not agree to any automatic renewal provisions because such agreements may violate the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1)(B). If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance), such license or service shall not renew automatically upon expiration of its current term without prior express Government approval by a warranted contracting officer.
Audit	Any clauses that give the Contractor the right to audit the government's use of software licenses do not meet the Government's needs as a matter of security. The Contractor can request that the Government conduct a self-audit and provide the Contractor with results of the audit, but the Contractor will not have access to the government's systems to conduct the audit.
Attorney fees and costs; equitable relief; arbitration	The Government does not agree to any clauses relating to the award of attorney's fees and costs or equitable relief because they may violate the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1)(B). Equitable relief and the award of attorney's fees, costs, or interest are only allowed to the extent permitted by statute (e.g., the Prompt Payment Act or Equal Access to Justice Act). Disputes will be resolved according to the disputes clause. Binding arbitration will not be used.
Taxes	The Government does not agree to any clauses purporting to make the Government responsible for all taxes. Any taxes the Contractor believes to be payable by the Government must be submitted individually to the JEDI Cloud Contracting Officer for adjudication or included in the firm-fixed price.
Incorporating other License Terms by Reference, Including Reference to a Website	Terms provided in other documents or websites do not bind the Government unless those terms are submitted with the proposal or in accordance with section H8 of the contract and made an attachment to the contract. Any license agreement provisions or terms of use unilaterally revised subsequent to award that are inconsistent with any material term or provision of this contract are not enforceable against the Government.

Venue; Choice of Law	The Government does not agree to any venue, jurisdiction, or choice of law clauses and does not consent to jurisdiction in any U.S. state courts. Venue and jurisdiction for any disputes are determined by the applicable federal statute (e.g., Contract Disputes Act) or by the Federal Acquisition Regulation. Any disputes arising under or related to this contract and license agreement will be governed by applicable federal statutes and regulations, not the laws of any particular U.S. state.
Arbitration	The Government does not agree to any provisions relating to mandatory arbitration. Disputes must be resolved in accordance with applicable federal statutes (e.g., Contract Disputes Act) and regulations.
Equitable remedies, injunctions	The Government does not agree to any clauses consenting to or entitling the Contractor to equitable relief or injunctions. Equitable relief for copyright, trademark, or patent infringement by the Government is only available to the extent permitted by federal statutes.
Unilateral termination by Contractor for breach	The Government does not agree to any clauses permitting unilateral termination of the contract or license agreement by the Contractor. Recourse against the United States for any alleged breach of this agreement must be made under the terms of the contract disputes clause (Contract Disputes Act). While a dispute is pending, the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and must comply with any decision of the Contracting Officer.
Unilateral modification	The Government does not agree to any provisions giving the Contractor the right to unilaterally change the license terms, with or without notice to the customer.

Assignment by licensor	The Government does not agree to any license terms providing for assignment by the licensor. Assignment of government contracts without the government's prior approval is prohibited by statute, except for assignment of payment to a financial institution, which must comply with the Assignment of Claims Act (31 U.S.C. § 3727, 41 U.S.C. § 15) and Federal Acquisition Regulation Subpart 32.8.
Confidentiality	The Government does not agree to any clauses asserting that unit prices or license agreement terms are confidential or proprietary information. Neither the license agreement nor the price list shall be deemed "confidential" or "proprietary" information notwithstanding any marking to that effect. The Freedom of Information Act (FOIA) governs what information must be disclosed and what information may be withheld by the Government.
References to External Sources (such as URL links)	The Government does not agree to any terms or conditions incorporated by reference to an external source if those terms or conditions are not in the agreement itself.

The Contractor agrees to all the terms of this Addendum and will abide by its provisions.

_____ _____
Signature of Authorized Representative Date

_____
Name of Authorized Representative

_____
Name of Contractor

(End of clause)

Section H9: Foreign Ownership, Control, or Influence

In each subcontract issued under this contract wherein any aspect of the subcontractor's work is classified, the Contractor shall include a requirement for Subcontractors to submit Foreign Ownership, Control, or Influence (FOCI) documentation to the JEDI Cloud Contracting Officer via the Defense Security Services (DSS) Electronic Facility Clearance System (e-FCL), just as the Contractor submits in DFARS clause 252.209-7002 via its certifications under FAR clause 52.204-7. The Contractor shall flowdown this clause.

Section H10: Online Marketplace Offerings

1. Integrated billing with the JEDI Cloud user's account is required for the JEDI Cloud online marketplace offerings.

2. With the exception of Bring Your Own License (BYOL), the Government's privity of contract for use of third party offerings remains with the Contractor. For such offerings, the Contractor agrees to the following:

a. To indemnify the Government against any third-party claim(s) related to the Government's alleged violation of a third-party license agreement where the term or condition at issue conflicts with the JEDI Cloud contract.

b. To ensure and validate that the online marketplace provisions third party offerings in a manner that is consistent with the third party's license agreement and take remedial action as necessary to resolve any issues.

3. For BYOL, the Government's privity of contract for the offering license agreement is with the third party. This does not negate the Contractor's responsibility to establish and maintain an online marketplace capable of deploying third party offerings IAW the Performance Work Statement.

a. The Contractor is not responsible for auditing or validating that the Government's use of BYOL offerings is consistent with the associated license agreement.

b. The license costs for BYOL offerings are not imputed against the JEDI Cloud contract maximum.

Section H11: Small Business Participation Commitment Document

Any modification to Attachment J-10 Small Business Participation Commitment Document must be pre-approved by the JEDI Cloud Contracting Officer prior to implementation.

SECTION I: CONTRACT CLAUSES

CLAUSES INCORPORATED BY REFERENCE

52.203-3	Gratuities	APR 1984
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-13	System for Award Management Maintenance	OCT 2016
52.212-4	Contract Terms And Conditions-- Commercial Items	MAY 2015
52.219-9	Small Business Subcontracting Plan	JAN 2017
52.219-16	Liquidated Damages -- Subcontracting Plan	JAN 1999
52.225-19	Contractor Personnel in a Designated Operational Area or Supporting a Diplomatic or Consular Mission Outside the United States	MAR 2008
52.232-1	Payments	APR 1984
52.232-8	Discounts For Prompt Payment	FEB 2002
52.232-17	Interest	MAY 2014
52.232-18	Availability Of Funds	APR 1984
52.232-23	Assignment Of Claims	MAY 2014
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.239-1	Privacy or Security Safeguards	AUG 1996
52.245-1	Government Property	APR 2012
52.245-1 Alt 1	Government Property, Alternate 1	APR 2012
52.245-9	Use and Charge	APR 2012
252.201-7000	Contracting Officer's Representative	DEC 1991
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.203-7003	Agency Office of the Inspector General	DEC 2012
252.204-7000	Disclosure Of Information	OCT 2016

252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7008	Compliance With Safeguarding Covered Defense Information Controls	OCT 2016
252.204-7009	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	OCT 2016
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	OCT 2016
252.204-7015	Notice of Authorized Disclosure of Information for Litigation Support	MAY 2016
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Country that is a State Sponsor of Terrorism	OCT 2015
252.211-7007	Reporting of Government Furnished Property	AUG 2012
252.219-7003	Small Business Subcontracting Plan (DOD Contracts)--Basic. (DEVIATION 2018-O0007)	MAR 2016
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7013	Rights In Technical Data--Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.227-7015	Technical Data--Commercial Items	FEB 2014
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7025	Limitations On The Use Or Disclosure Of Government-furnished Information Marked With Restrictive Legends	MAY 2013
252.227-7019	Validation of Asserted Restrictions--Computer Software	SEP 2016
252.227-7027	Deferred Ordering of Technical Data or Computer Software	APR 1988
252.227-7030	Technical Data--Withholding Of Payment	MAR 2000
252.227-7037	Validation of Restrictive Markings on Technical Data	SEP 2016
252.232-7010	Levies on Contract Payments	DEC 2006
252.239-7010	Cloud Computing Services	OCT 2016
252.239-7018	Supply Chain Risk	OCT 2015
252.243-7001	Pricing Of Contract Modifications	DEC 1991

252.243-7002	Requests for Equitable Adjustment	DEC 2012
252.244-7000	Subcontracts for Commercial Items	JUN 2013
252.245-7001	Tagging, Labeling and Marking of Government Furnished Property	APR 2012
252.245-7002	Reporting Loss of Government Property	APR 2012
252.245-7003	Contractor Property Management System Administration	APR 2012
252.245-7004	Reporting, Reutilization, and Disposal	SEP 2016
252.247-7023	Transportation of Supplies by Sea	APR 2014

CLAUSES INCORPORATED BY FULL TEXT

52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) *Definitions*. As used in this clause--
"Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.
"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).
"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
"Safeguarding" means measures or controls that are prescribed to protect information systems.
(b) Safeguarding requirements and procedures.
(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(iii) Verify and control/limit connections to and use of external information systems.
(iv) Control information posted or processed on publicly accessible information systems.
(v) Identify information system users, processes acting on behalf of users, or devices.
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(xii) Identify, report, and correct information and information system flaws in a timely manner.
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
(xiv) Update malicious code protection mechanisms when new releases are available.
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements*. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (DEVIATION 2013-O0019) (SEP 2013)

(a) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (a) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records—Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(b) (1) Notwithstanding the requirements of any other clauses of this contract, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (b) (1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).

(ii) 52.219-8, Utilization of Small Business Concerns (Dec 2010) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
(iii) 52.222-17, Nondisplacement of Qualified Workers (JAN 2013) (E.O. 13495). Flow down required in accordance with paragraph (l) of FAR clause 52.222-17.
(iv) 52.222-26, Equal Opportunity (Mar 2007) (E.O. 11246).
(v) 52.222-35, Equal Opportunity for Veterans (Sep 2010) (38 U.S.C. 4212).
(vi) 52.222-36, Affirmative Action for Workers with Disabilities (Oct 2010) (29 U.S.C. 793).
(vii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C .Chapter 67).
(ix) 52.222-50, Combating Trafficking in Persons (Feb 2009) (22 U.S.C. 7104(g)).
Alternate I (Aug 2007) of 52.222-50 (22 U.S.C. 7104(g)).
(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (Nov 2007) (41 U.S.C. Chapter 67).
(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services-Requirements (Feb 2009) (41 U.S.C. Chapter 67).
(xii) 52.222-54, Employment Eligibility Verification (E.O. 12989) (JUL 2012).
(xiii) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
(xiv) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Mar 2009) 42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
(xv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.
(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or TOs by the individuals or activities designated in the Schedule. Such orders may be issued from the applicable period of performance, April 17, 2019 through April 16, 2029, if all options are exercised as follows:

Base Period =April 17, 2019 through April 16, 2021
Option Period 1 = April 17, 2021 through April 16, 2024
Option Period 2 = April 17, 2024 through April 16, 2027
Option Period 3 = April 17, 2027 through April 16, 2029

(b) All delivery orders or TOs are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or TO and this contract, the contract shall control.
(c) If mailed, a delivery order or TO is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of Clause)

52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) *Minimum order.* When the Government requires supplies or services covered by this contract in an amount of less than $1,000.00*,* the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.
(b) *Maximum order*. The Contractor is not obligated to honor --
(1) Any order for a single item in excess of $1,000,000,000.00;
(2) Any order for a combination of items in excess of $1,000,000,000.00; or
(3) A series of orders from the same ordering office within 90 days that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) of this section.
(c) If this is a requirements contract (*i.e.*, includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.
(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 7 calendar days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.
(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."
(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.
(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after **April 16, 2030.**

(End of Clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 31 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

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

exceed 120 months.

(End of clause)

52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond September 30, 2019 (and is understood by the contractor to be updated with the appropriate fiscal year). The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond September 30, 2019, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browsefar

https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

(End of clause)

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation (48 CFR 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

SECTION J: LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

a. Exhibits applicable to this contract are identified as follows:

Documents requested in this RFP are subject the Contract Data Requirements List (CDRL) detailed in Exhibit A below and are appended as Attachment J-9 of the RFP.

Exhibit A	
CDRL Number	**Title**

A001	Contract Monthly Progress Report (CMPR)
A002	Transition Out Plan
A003	Contract Security Management Plan
A004	Technology Refresh Plan
A005	System Administrator Training Materials
A006	Role-Based User Training Materials
A007	Portability Plan
A008	Contract Ordering Guide
A009	Change Management Roadmap
A010	Quality Control Plan
A011	Security Authorization Package
A012	Technical Report
A013	Small Business Reporting
A014	Portability Test
A015	Task Order Monthly Progress Report
A016	Meeting Materials

b. The following attachments will be incorporated into the awarded contract:

J-1: Price Catalogs
J-2: PWS for ID/IQ
J-3: Contractor Discounts, Premiums, and Fees
J-4: Small Business Subcontracting Plan
J-5: Licenses and Service Level Agreements
J-6: JEDI Cloud Cyber Security Plan
J-7: DD Form 254, DoD Contract Security Classification Specification for ID/IQ
J-8: Definitions
J-9: Contract Data Requirements Lists (CDRLs)
J-10: Small Business Participation Commitment Document

SECTION K: REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS

CLAUSES INCORPORATED BY REFERENCE

52.209-2	Prohibition on Contracting with Inverted Domestic Corporations--Representation	NOV 2015
52.222-56	Certification Regarding Trafficking in Persons Compliance Plan.	MAR 2015
252.203-7005	Representation Relating to Compensation of Former DoD Officials	NOV 2011
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	JUN 1995
252.239-7009	Representation of Use of Cloud Computing	SEP 2015

CLAUSES INCORPORATED BY FULL TEXT

52.203-2 CERTIFICATE OF INDEPENDENT PRICE DETERMINATION (APR 1985)

(a) The offeror certifies that --
(1) The prices in this offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to –
(i) Those prices,
(ii) The intention to submit an offer, or
(iii) The methods of factors used to calculate the prices offered:
(2) The prices in this offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a sealed bid solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law; and
(3) No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.
(b) Each signature on the offer is considered to be a certification by the signatory that the signatory --
(1) Is the person in the offeror's organization responsible for determining the prices offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision; or
(2) (i) Has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision
_____ (insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization);
(ii) As an authorized agent, does certify that the principals named in subdivision (b)(2)(i) above have not participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) above; and
(iii) As an agent, has not personally participated, and will not participate, in any action contrary to subparagraphs (a)(1) through (a)(3) of this provision.
(c) If the offeror deletes or modifies subparagraph (a)(2) of this provision, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.
(End of clause)

52.204-20 PREDECESSOR OF OFFEROR (JUL 2016)

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

Commercial and Government Entity (CAGE) code means--
(1) An identifier assigned to entities located in the United States or its outlying areas by the Defense Logistics Agency (DLA) Commercial and Government Entity (CAGE) Branch to identify a commercial or government entity; or
(2) An identifier assigned by a member of the North Atlantic Treaty Organization (NATO) or by the NATO Support and Procurement Agency (NSPA) to entities located outside the United States and its outlying areas that the DLA Commercial and Government Entity (CAGE) Branch records and maintains in the CAGE master file. This type of
code is known as a NATO CAGE (NCAGE) code.
Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.
Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.
(b) The Offeror represents that it [____] is or [____] is not a successor to a predecessor that held a Federal contract or grant within the last three years.
(c) If the Offeror has indicated "is" in paragraph (b) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):
Predecessor CAGE code: ____ (or mark "Unknown").
Predecessor legal name: ____.
(Do not use a "doing business as" name).
(End of provision)

52.209-7 INFORMATION REGARDING RESPONSIBILITY MATTERS (JULY 2013)

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

Administrative proceeding means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.
Federal contracts and grants with total value greater than $10,000,000 means--
(1) The total value of all current, active contracts and grants, including all priced options; and
(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).
Principal means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).
(b) The Offeror ( ) has ( ) does not have current active Federal contracts and grants with total value greater than $10,000,000.
(c) If the Offeror checked "has" in paragraph (b) of this provision, the Offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission

of this offer with regard to the following information:
(1) Whether the Offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the Offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:
(i) In a criminal proceeding, a conviction.
(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.
(iii) In an administrative proceeding, a finding of fault and liability that results in--
(A) The payment of a monetary fine or penalty of $5,000 or more; or
(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.
(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.
(2) If the Offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the Offeror has provided the requested information with regard to each occurrence.
(d) The Offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management database via https://www.acquisition.gov (see 52.204-7).

(End of provision)

52.209-11 REPRESENTATION BY CORPORATIONS REGARDING DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (FEB 2016)

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that--

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or
(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that—

(1) It is [ ] is not [ ] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and
(2) It is [ ] is not [ ] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS--COMMERCIAL ITEMS (DEC 2016)

The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the

annual representations and certification electronically via the System for Award Management (SAM) Web site located at https://www.sam.gov/portal. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (t) of this provision.

(a) Definitions. As used in this provision --
"Administrative merits determination" means certain notices or findings of labor law violations issued by an enforcement agency following an investigation. An administrative merits determination may be final or be subject to appeal or further review. To determine whether a particular notice or finding is covered by this definition, it is necessary to consult section II.B. in the DOL Guidance.
"Arbitral award or decision" means an arbitrator or arbitral panel determination that a labor law violation occurred, or that enjoined or restrained a violation of labor law. It includes an award or decision that is not final or is subject to being confirmed, modified, or vacated by a court, and includes an award or decision resulting from private or confidential proceedings. To determine whether a particular award or decision is covered by this definition, it is necessary to consult section II.B. in the DOL Guidance.

"Civil judgment" means—

- In paragraph (h) of this provision: A judgment or finding of a civil offense by any court of competent jurisdiction.

(2) In paragraph (s) of this provision: Any judgment or order entered by any Federal or State court in which the court determined that a labor law violation occurred, or enjoined or restrained a violation of labor law. It includes a judgment or order that is not final or is subject to appeal. To determine whether a particular judgment or order is covered by this definition, it is necessary to consult section II.B. in the DOL Guidance.
"DOL Guidance" means the Department of Labor (DOL) Guidance entitled: ``Guidance for Executive Order 13673, `Fair Pay and Safe Workplaces' ". The DOL Guidance, dated August 25, 2016, can be obtained from www.dol.gov/fairpayandsafeworkplaces.
"Economically disadvantaged women-owned small business (EDWOSB) Concern" means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.
"Enforcement agency" means any agency granted authority to enforce the Federal labor laws. It includes the enforcement components of DOL (Wage and Hour Division, Office of Federal Contract Compliance Programs, and Occupational Safety and Health Administration), the Equal Employment Opportunity Commission, the Occupational Safety and Health Review Commission, and the National Labor Relations Board. It also means a State agency designated to administer an OSHA-approved State Plan, but only to the extent that the State agency is acting in its capacity as administrator of such plan. It does not include other Federal agencies which, in their capacity as contracting agencies, conduct investigations of potential labor law violations. The enforcement agencies associated with each labor law under E.O. 13673
are--

(1) Department of Labor Wage and Hour Division (WHD) for--
(i) The Fair Labor Standards Act;
(ii) The Migrant and Seasonal Agricultural Worker Protection Act;
(iii) 40 U.S.C. chapter 31, subchapter IV, formerly known as the Davis-Bacon Act;
(iv) 41 U.S.C. chapter 67, formerly known as the Service Contract Act;
(v) The Family and Medical Leave Act; and
(vi) E.O. 13658 of February 12, 2014 (Establishing a Minimum Wage for Contractors);

(2) Department of Labor Occupational Safety and Health Administration (OSHA) for-
(i) The Occupational Safety and Health Act of 1970; and
(ii) OSHA-approved State Plans;
(3) Department of Labor Office of Federal Contract Compliance Programs (OFCCP) for--
(i) Section 503 of the Rehabilitation Act of 1973;
(ii) The Vietnam Era Veterans' Readjustment Assistance Act of 1972 and the Vietnam Era Veterans' Readjustment Assistance Act of 1974; and
(iii) E.O. 11246 of September 24, 1965 (Equal Employment Opportunity);
(4) National Labor Relations Board (NLRB) for the National Labor Relations Act; and
(5) Equal Employment Opportunity Commission (EEOC) for--
(i) Title VII of the Civil Rights Act of 1964;
(ii) The Americans with Disabilities Act of 1990;
(iii) The Age Discrimination in Employment Act of 1967; and
(iv) Section 6(d) of the Fair Labor Standards Act (Equal Pay Act).

"Forced or indentured child labor" means all work or service-

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or
(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

“Highest-level owner” means the entity that owns or controls an immediate owner of the Offeror, or that owns or controls one or more entities that control an immediate owner of the Offeror. No entity owns or exercises control of the highest level owner.
“Immediate owner” means an entity, other than the Offeror, that has direct control of the Offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.
“Inverted domestic corporation” means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).
“Labor compliance agreement” means an agreement entered into between a contractor or subcontractor and an enforcement agency to address appropriate remedial measures, compliance assistance, steps to resolve issues to increase compliance with the labor laws, or other related matters.

“Labor laws” means the following labor laws and E.O.s:

(1) The Fair Labor Standards Act.

(2) The Occupational Safety and Health Act (OSHA) of 1970.

(3) The Migrant and Seasonal Agricultural Worker Protection Act.

(4) The National Labor Relations Act.

(5) 40 U.S.C. chapter 31, subchapter IV, formerly known as the Davis-Bacon Act.

(6) 41 U.S.C. chapter 67, formerly known as the Service Contract Act.

(7) E.O. 11246 of September 24, 1965 (Equal Employment Opportunity).

(8) Section 503 of the Rehabilitation Act of 1973.

(9) The Vietnam Era Veterans' Readjustment Assistance Act of 1972 and the Vietnam Era Veterans' Readjustment Assistance Act of 1974.

(10) The Family and Medical Leave Act.

(11) Title VII of the Civil Rights Act of 1964.

(12) The Americans with Disabilities Act of 1990.

(13) The Age Discrimination in Employment Act of 1967.

(14) E.O. 13658 of February 12, 2014 (Establishing a Minimum Wage for Contractors).

(15) Equivalent State laws as defined in the DOL Guidance. (The only equivalent State laws implemented in the FAR are OSHA-approved State Plans, which can be found at www.osha.gov/dcsp/osp/approved_state_plans.html).

“Labor law decision” means an administrative merits determination, arbitral award or decision, or civil judgment, which resulted from a violation of one or more of the laws listed in the definition of ``labor laws''.

“Manufactured end product” means any end product in product and service codes (PSCs) 1000-9999, except--

(1) PSC 5510, Lumber and Related Basic Wood Materials;

(2) Product or Service Group (PSG) 87, Agricultural Supplies;

(3) PSG 88, Live Animals;

(4) PSG 89, Subsistence;

(5) PSC 9410, Crude Grades of Plant Materials;

(6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;

(7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;

(8) PSC 9610, Ores;

(9) PSC 9620, Minerals, Natural and Synthetic; and

(10) PSC 9630, Additive Metal Materials.

“Place of manufacture” means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

“Predecessor” means an entity that is replaced by a successor and includes any predecessors of the predecessor.

“Restricted business operations” means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the

business can demonstrate--

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;
(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;
(3) Consist of providing goods or services to marginalized populations of Sudan;
(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;
(5) Consist of providing goods or services that are used only to promote health or education; or
(6) Have been voluntarily suspended.

Sensitive technology--

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically--
(i) To restrict the free flow of unbiased information in Iran; or
(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and
(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

Service-disabled veteran-owned small business concern--

(1) Means a small business concern--
(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and
(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.
(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).
"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.
“Small disadvantaged business concern”, consistent with 13 CFR 124.1002, means a small business concern under the size standard applicable to the acquisition, that--
(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by--
(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and
(ii) Each individual claiming economic disadvantage has a net worth not exceeding $750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and
(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.
“Subsidiary” means an entity in which more than 50 percent of the entity is owned--

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

“Successor” means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term “successor” does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

“Veteran-owned small business concern” means a small business concern--

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

"Women-owned business concern" means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

"Women-owned small business concern" means a small business concern--

(1) That is at least 51 percent owned by one or more women or, in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; or

(2) Whose management and daily business operations are controlled by one or more women.

“Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127)”, means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.
Note to paragraph (a): By a court order issued on October 24, 2016, the following definitions in this paragraph (a) are enjoined indefinitely as of the date of the order: ``Administrative merits determination", ``Arbitral award or decision", paragraph (2) of ``Civil judgment", ``DOL Guidance", ``Enforcement agency", ``Labor compliance agreement", ``Labor laws", and ``Labor law decision". The enjoined definitions will become effective immediately if the court terminates the injunction. At that time, DoD, GSA, and NASA will publish a document in the Federal Register advising the public of the termination of the injunction.

(b) (1) Annual Representations and Certifications. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications posted electronically on the SAM website.

(2) The Offeror has completed the annual representations and certifications electronically via the SAM website accessed through https://www.acquisition.gov. After reviewing the SAM database information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications--Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs ___ .

[Offeror to identify the applicable paragraphs at (c) through (t) of this provision that the Offeror has completed for the purposes of this solicitation only, if any.) These amended representation(s) and/or

certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the Offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted electronically on ORCA.]

(c) Offerors must complete the following representations when the resulting contract will be performed in the United States or its outlying areas. Check all that apply.

(1) Small business concern. The Offeror represents as part of its offer that it (___) is, (___) is not a small business concern.

(2) Veteran-owned small business concern. (Complete only if the Offeror represented itself as a small business concern in paragraph (c)(1) of this provision.) The Offeror represents as part of its offer that it (___) is, (___) is not a veteran-owned small business concern.

(3) Service-disabled veteran-owned small business concern. (Complete only if the Offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.) The Offeror represents as part of its offer that it (___) is, (___) is not a service-disabled veteran-owned small business concern.

(4) Small disadvantaged business concern. (Complete only if the Offeror represented itself as a small business concern in paragraph (c)(1) of this provision.) The Offeror represents that it (___) is, (___) is not a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) Women-owned small business concern. (Complete only if the Offeror represented itself as a small business concern in paragraph (c)(1) of this provision.) The Offeror represents that it (___) is, (___) is not a women-owned small business concern.

Note to paragraphs (c)(8) and (9): Complete paragraphs (c)(8) and (c)(9) only if this solicitation is expected to exceed the simplified acquisition threshold.

(6) WOSB concern eligible under the WOSB Program. [Complete only if the Offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The Offeror represents that--

(i) It [___] is, [___] is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have
been issued that affects its eligibility; and

(ii) It [___] is, [___] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. [The Offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture: ___ .] Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the Offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.] The Offeror represents that--

(i) It [___] is, [___] is not an EDWOSB concern, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects

its eligibility; and

(ii) It [___] is, [___] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. [The Offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture: ___ -.] Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

(8) Women-owned business concern (other than small business concern). (Complete only if the Offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.) The Offeror represents that it (___) is, a women-owned business concern.

(9) Tie bid priority for labor surplus area concerns. If this is an invitation for bid, small business Offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by Offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

___

(10) HUBZone small business concern. (Complete only if the Offeror represented itself as a small business concern in paragraph (c)(1) of this provision.) The Offeror represents, as part of its offer, that--

(i) It [___] is, [___] is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material changes in ownership and control, principal office, or HUBZone employee percentage have occurred since it was certified in accordance with 13 CFR Part 126; and

(ii) It [___] is, [___] is not a HUBZone joint venture that complies with the requirements of 13 CFR Part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for each HUBZone small business concern participating in the HUBZone joint venture. [The Offeror shall enter the names of each of the HUBZone small business concerns participating in the HUBZone joint venture: ___ .] Each HUBZone small business concern participating in the HUBZone joint venture shall submit a separate signed copy of the HUBZone representation.

(d) Certifications and representations required to implement provisions of Executive Order 11246--

(1) Previous Contracts and Compliance. The Offeror represents that--

(i) It (___) has, (___) has not, participated in a previous contract or subcontract subject either to the Equal Opportunity clause of this solicitation, the and

(ii) It (___) has, (___) has not, filed all required compliance reports.

(2) Affirmative Action Compliance. The Offeror represents that--

(i) It (___) has developed and has on file, (___) has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR Subparts 60-1 and 60-2), or

(ii) It (___) has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) Certification Regarding Payments to Influence Federal Transactions (31 U.S.C. 1352). (Applies only if the contract is expected to exceed $150,000.) By submission of its offer, the Offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the Offeror with respect to this contract, the Offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The Offeror need not report regularly employed officers or employees of the Offeror to whom payments of reasonable compensation were made.

(f) Buy American Certificate. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American --Supplies, is included in this solicitation.)

(1) The Offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the Offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The Offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of “domestic end product.” The terms “commercially available off-the-shelf (COTS) item,” “component,” “domestic end product,” “end product,” “foreign end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American--Supplies.”

(2) Foreign End Products:

Line Item No.	Country of Origin
___	___
___	___
___	___

(List as necessary)

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g)(1) Buy American--Free Trade Agreements--Israeli Trade Act Certificate. (Applies only if the clause at FAR 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act, is included in this solicitation.)

(i) The Offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that for other than COTS items, the Offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms ``Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end product,'' ``commercially available off-the-shelf (COTS) item,'' ``component,'' ``domestic end product,'' ``end product,'' ``foreign end product,'' ``Free Trade Agreement country,'' ``Free Trade Agreement country end product,'' ``Israeli end product,'' and ``United States'' are defined in the clause of this solicitation entitled ``Buy American--Free Trade Agreements--Israeli Trade Act.''

(ii) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled ``Buy American--Free Trade Agreements--Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
___	___
___	___
___	___

[List as necessary]

(iii) The Offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act." The Offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of “domestic end product.”

Other Foreign End Products:

Line Item No.	Country of Origin
___	___
___	___

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American Act-Free Trade Agreements-Israeli Trade Act Certificate, Alternate I (Jan 2004)*. If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The Offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American -Free Trade Agreements-Israeli Trade Act":

Canadian End Products:

Line Item No.
___
___
___

[List as necessary]

(3) Buy American-Free Trade Agreements-Israeli Trade Act Certificate, Alternate II (Jan 2004). If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The Offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled "Buy American-Free Trade Agreements-Israeli Trade Act":

Canadian or Israeli End Products:

Line Item No.	Country of Origin
___	___
___	___
___	___

[List as necessary]

(4) Buy American--Free Trade Agreements--Israeli Trade Act Certificate, Alternate III. If Alternate III to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The Offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled ``Buy American --Free Trade Agreements--Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
___	___
___	___

[List as necessary]

(5) Trade Agreements Certificate. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The Offeror certifies that each end product, except those listed in paragraph (g)(5)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled ``Trade Agreements".

(ii) The Offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products:

Line Item No.	Country of Origin
___	___
___	___

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters (Executive Order 12689)*. (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The Offeror certifies, to the best of its knowledge and belief, that the Offeror and/or any of its principals--
(1) [___] Are, [___] are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;
(2) [___] Have, [___] have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property; and
(3) [___] Are, [___] are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and
(4) [___] Have, [___] have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds $3,500 for which the liability remains unsatisfied.
(i) Taxes are considered delinquent if both of the following criteria apply:
(A) *The tax liability is finally determined.* The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.
(B) *The taxpayer is delinquent in making payment.* A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.
(ii) Examples.
(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appear rights.
(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals Contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.
(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.
(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. §362 (the Bankruptcy Code).

(i) Certification Regarding Knowledge of Child Labor for *Listed End Products (Executive Order 13126)*. [*The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at* 22.1503*(b)*.]

(1) *Listed end products*.

Listed End Product	Listed Countries of Origin
___	___
___	___

(2) *Certification*. [*If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the Offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.*]

[___] (i) The Offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

[___] (ii) The Offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The Offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the Offeror certifies that it is not aware of any such use of child labor.
(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the Offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—
(1) (___) In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or
(2) (___) Outside the United States.

(j) Place of manufacture. (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the Offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly--
(1) (___) In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or
(2) (___) Outside the United States.

(k) Certificates regarding exemptions from the application of the Service Contract Labor Standards. (Certification by the Offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.)

[The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]

[___] (1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The Offeror (___) does (___) does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the Offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;
(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

[___] (2) Certain services as described in FAR 22.1003-4(d)(1). The Offeror (___) does (___) does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the Offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;
(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));
(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and
(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.
(3) If paragraph (k)(1) or (k)(2) of this clause applies—
(i) If the Offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the Offeror shall notify the Contracting Officer as soon as possible; and
(ii) The Contracting Officer may not make an award to the Offeror if the Offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.
(l) Taxpayer Identification Number (TIN) (26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the Offeror is required to provide this information to the SAM database to be eligible for award.)
(1) All Offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).
(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the Offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the Offeror's TIN.
(3) Taxpayer Identification Number (TIN).

(___) TIN: ----------.

(___) TIN has been applied for.

(___) TIN is not required because:

(___) Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

(___) Offeror is an agency or instrumentality of a foreign government;

(___) Offeror is an agency or instrumentality of the Federal Government.

(4) Type of organization.

(___) Sole proprietorship;

(___) Partnership;

(___) Corporate entity (not tax-exempt);

(___) Corporate entity (tax-exempt);

(___) Government entity (Federal, State, or local);

(___) Foreign government;

(___) International organization per 26 CFR 1.6049-4;

(___) Other ----------.

(5) Common parent.

(___) Offeror is not owned or controlled by a common parent;

(___) Name and TIN of common parent:

Name - _____ .
TIN - _____ .

(m) Restricted business operations in Sudan. By submission of its offer, the Offeror certifies that the Offeror does not conduct any restricted business operations in Sudan.
(n) Prohibition on Contracting with Inverted Domestic Corporations—

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) Representation. By submission of its offer, the Offeror represents that--

(i) It is not an inverted domestic corporation; and

(ii) It is not a subsidiary of an inverted domestic corporation.

(o) Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.

(1) The Offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(2) Representation. The Offeror represents that--

(i) It [___] is, [___] is not an inverted domestic corporation; and

(ii) It [___] is, [___] is not a subsidiary of an inverted domestic corporation.

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if—

(i) This solicitation includes a trade agreements certification (e.g., 52.212-3(g) or a comparable agency provision); and

(ii) The Offeror has certified that all the offered products to be supplied are designated country end products.

(p) *Ownership or Control of Offeror*. (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation.
(1) The Offeror represents that it [___] has or [___] does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.
(2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:
Immediate owner CAGE code: ___
Immediate owner legal name: ___
(Do not use a "doing business as" name)
Is the immediate owner owned or controlled by another entity:
[___] Yes or [___] No.
(3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:
Highest level owner CAGE code: ___
Highest level owner legal name: ___
(Do not use a "doing business as" name)
(q) *Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.*
(1) As required by section 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that—
(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless and agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or
(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.
(2) The Offeror represents that--

(i) It is [___] is not [___] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and
(ii) It is [___] is not [___] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.
(r) Predecessor of Offeror. (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it [___] is or [___] is not a successor to a predecessor that held a Federal contract or grant within the last three years.
(2) If the Offeror has indicated ``is'' in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: ___ (or mark ``Unknown'').

Predecessor legal name: ___ .

(Do not use a ``doing business as'' name).

(s) Representation regarding compliance with labor laws (Executive Order 13673). If the Offeror is a joint venture that is not itself a separate legal entity, each concern participating in the joint venture shall separately comply with the requirements of this provision.

(1)(i) For solicitations issued on or after October 25, 2016 through April 24, 2017: The Offeror [___] does [___] does not anticipate submitting an offer with an estimated contract value of greater than $50 million.

(ii) For solicitations issued after April 24, 2017: The Offeror [___] does [___] does not anticipate submitting an offer with an estimated contract value of greater than $500,000.

(2) If the Offeror checked ``does'' in paragraph (s)(1)(i) or (ii) of this provision, the Offeror represents to the best of the Offeror's knowledge and belief [Offeror to check appropriate block]:

[___](i) There has been no administrative merits determination, arbitral award or decision, or civil judgment for any labor law violation(s) rendered against the Offeror (see definitions in paragraph (a) of this section) during the period beginning on October 25, 2015 to the date of the offer, or for three years preceding the date of the offer, whichever period is shorter; or

[___](ii) There has been an administrative merits determination, arbitral award or decision, or civil judgment for any labor law violation(s) rendered against the Offeror during the period beginning on October 25, 2015 to the date of the offer, or for three years preceding the date of the offer, whichever period is shorter.

(3)(i) If the box at paragraph (s)(2)(ii) of this provision is checked and the Contracting Officer has initiated a responsibility determination and has requested additional information, the Offeror shall provide--

(A) The following information for each disclosed labor law decision in the System for Award Management (SAM) at www.sam.gov, unless the information is already current, accurate, and complete in SAM. This

information will be publicly available in the Federal Awardee Performance and Integrity Information System (FAPIIS):

(1) The labor law violated.

(2) The case number, inspection number, charge number, docket number, or other unique identification number.

(3) The date rendered.

(4) The name of the court, arbitrator(s), agency, board, or commission that rendered the determination or decision;

(B) The administrative merits determination, arbitral award or decision, or civil judgment document, to the Contracting Officer, if the Contracting Officer requires it;

(C) In SAM, such additional information as the Offeror deems necessary to demonstrate its responsibility, including mitigating factors and remedial measures such as Offeror actions taken to address the violations, labor compliance agreements, and other steps taken to achieve compliance with labor laws. Offerors may provide explanatory text and upload documents. This information will not be made public unless the contractor determines that it wants the information to be made public; and

(D) The information in paragraphs (s)(3)(i)(A) and (s)(3)(i)(C) of this provision to the Contracting Officer, if the Offeror meets an exception to SAM registration (see FAR 4.1102(a)).

(ii)(A) The Contracting Officer will consider all information provided under (s)(3)(i) of this provision as part of making a responsibility determination.

(B) A representation that any labor law decision(s) were rendered against the Offeror will not necessarily result in withholding of an award under this solicitation. Failure of the Offeror to furnish a representation or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(C) The representation in paragraph (s)(2) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous representation, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation in accordance with the procedures set forth in FAR 12.403.

(4) The Offeror shall provide immediate written notice to the Contracting Officer if at any time prior to contract award the Offeror learns that its representation at paragraph (s)(2) of this provision is no longer accurate.

(5) The representation in paragraph (s)(2) of this provision will be public information in the Federal Awardee Performance and Integrity Information System (FAPIIS).

Note to paragraph (s): By a court order issued on October 24, 2016, this paragraph (s) is enjoined indefinitely as of the date of the order. The enjoined paragraph will become effective immediately if the court terminates the injunction. At that time, DoD, GSA, and NASA will publish a document in the Federal Register advising the public of the termination of the injunction.

(t) Public Disclosure of Greenhouse Gas Emissions and Reduction Goals. Applies in all solicitations that require Offerors to register in SAM (52.212-1(k)).

(1) This representation shall be completed if the Offeror received $7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than $7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)]. (i) The Offeror (itself or through its immediate owner or highest-level owner) [___] does, [___] does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible Web site the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) [___] does, [___] does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible Web site a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible Web site includes the Offeror's own Web site or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked ``does'' in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible Web site(s) where greenhouse gas emissions and/or reduction goals are reported: ___ .
(End of provision)

52.222-22 PREVIOUS CONTRACTS AND COMPLIANCE REPORTS (FEB 1999)

The Offeror represents that --
(a) ( ) It has, ( ) has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation;
(b) ( ) It has, ( ) has not, filed all required compliance reports; and
(c) Representations indicating submission of required compliance reports, signed by proposed subcontractors, will be obtained before subcontract awards.

(End of provision)

252.209-7999 REPRESENTATION BY CORPORATIONS REGARDING AN UNPAID DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW (DEVIATION 2012-O0004) (JAN 2012)

(a) In accordance with sections 8124 and 8125 of Division A of the Consolidated Appropriations Act, 2012,(Pub. L. 112-74) none of the funds made available by that Act may be used to enter into a contract with any corporation that—
(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government.
(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered

suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.
(b) The Offeror represents that—

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

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

(End of provision)

252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JAN 2011)

(a) The terms used in this provision are defined in following clause or clauses contained in this solicitation—

(1) If a successful offeror will be required to deliver technical data, the Rights in Technical Data--Noncommercial Items clause, or, if this solicitation contemplates a contract under the Small Business Innovation Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause.
(2) If a successful offeror will not be required to deliver technical data, the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause, or, if this solicitation contemplates a contract under the Small Business Innovation Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program clause.

(b) The identification and assertion requirements in this provision apply only to technical data, including computer software documentation, or computer software to be delivered with other than unlimited rights. For contracts to be awarded under the Small Business Innovation Research Program, the notification and identification requirements do not apply to technical data or computer software that will be generated under the resulting contract. Notification and identification is not required for restrictions based solely on copyright.
(c) Offers submitted in response to this solicitation shall identify, to the extent known at the time an offer is submitted to the Government, the technical data or computer software that the Offeror, its subcontractors or suppliers, or potential subcontractors or suppliers, assert should be furnished to the Government with restrictions on use, release, or disclosure.
(d) The Offeror's assertions, including the assertions of its subcontractors or suppliers or potential subcontractors or suppliers, shall be submitted as an attachment to its offer in the following format, dated and signed by an official authorized to contractually obligate the Offeror:

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software.

The Offeror asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted:

Technical Data or			
Computer Software			Name of Person

to be Furnished	Basis for	Asserted Rights	Asserting
With Restrictions*	Assertion**	Category***	Restrictions****
(LIST)*****	(LIST)	(LIST)	(LIST)

*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation identify the software or documentation.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., government purpose license rights from a prior contract, rights in SBIR data generated under another contract, limited, restricted, or government purpose rights under this or a prior contract, or specially negotiated licenses).

****Corporation, individual, or other person, as appropriate.

*****Enter “none” when all data or software will be submitted without restrictions.

Date _____

Printed Name and Title _____

_____

Signature _____

(End of identification and assertion)

(e) An offeror's failure to submit, complete, or sign the notification and identification required by paragraph (d) of this provision with its offer may render the offer ineligible for award.

(f) If the Offeror is awarded a contract, the assertions identified in paragraph (d) of this provision shall be listed in an attachment to that contract. Upon request by the Contracting Officer, the Offeror shall provide sufficient information to enable the Contracting Officer to evaluate any listed assertion.

(End of provision)

SECTION L: INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

Section L1: General RFP Instructions

This section of the RFP provides guidance and information for preparing proposals, as well as instructions on the format and content of the proposal. The Offeror shall submit a complete proposal including all data and information requested by the RFP. The proposal must be submitted IAW all Section L instructions.

Any estimates, examples, or scenarios included in Section L are based on the Government's projected needs and are used for evaluation purposes only. These estimates do not represent a guarantee for any TOs placed against the resulting contract. RFP Section B2 includes the minimum guaranteed award amount.

The following attachments are hereby incorporated into combined synopsis/solicitation # HQ0034-18-R-0077. These attachments are for the RFP only and will not be attached to the awarded ID/IQ contract. For clarity, Attachments L-3 and L-4 will be awarded as TOs concurrently with the ID/IQ contract award.

L-1: JEDI Cloud SOO
L-2: Price Scenarios
L-3: TO 001 PWS
L-4: TO 002 PWS
L-5: Price Scenario Price Build-Up Template
L-6: Small Business Subcontracting Plan Template
L-7: OCI Analysis/Disclosure Form
L-8: PWS/SOO & Factor Crosswalk Matrix
L-9: Company Non-Disclosure Agreement for JEDI Cloud

1. The Government anticipates awarding a single ID/IQ contract, for the JEDI Cloud, to the responsive and responsible Offeror whose proposal represents the best value to the Government as set forth in Section M - Evaluation For Award Of ID/IQ Contract and Task Orders detailed below. This RFP is issued for full and open competition.

2. The Government anticipates issuing two TOs to the awardee concurrently with the JEDI Cloud ID/IQ contract award. The Offeror shall address the PWS requirements for TO 001, provided in Attachment L-3 to this RFP, IAW the RFP instructions. The Offeror's proposal for TO 001 will be evaluated IAW Section M - Evaluation For Award Of ID/IQ Contract and Task Orders. TO 002, provided in Attachment L-4 of the RFP, is for administrative purposes only to obligate the ID/IQ contract minimum guarantee in Section B2 of the RFP. Additional explanation is provided in Attachment L-4.

3. The Government intends to conduct discussions for this acquisition, but reserves the right to forego discussions with Offerors. IAW FAR 52.215-1, ALT I, pursuant to the stipulated conditions, the JEDI Cloud Contracting Officer may limit the number of proposals in the competitive range to the greatest number that will permit an efficient competition among the most highly rated proposals. The competitive range will be limited to no more than four proposals. Additionally, IAW FAR Part 15.306(c)(2), Offerors are advised that the competitive range may be further reduced for purposes of efficiency. As such, the Offeror's initial offer should contain its best terms from a price and technical standpoint.

4. The Government may consider any failure to comply with these instructions to be indicative of what could be expected from an Offeror during contract performance and may consider it a

weakness of the proposal.

5. The proposal shall be clear, concise, and shall include sufficient detail for effective evaluation and for substantiating the validity of stated claims. The proposal should not simply rephrase or restate the Government's requirements but rather shall provide convincing rationale to address how the Offeror intends to meet these requirements. Statements such as "will comply," "noted and understood," "in accordance with best industry practices/standards," etc., without supporting narrative are unacceptable. Offerors shall assume that the Government has no prior knowledge of their capabilities and experience and will base its evaluation solely on the information presented in the Offeror's proposal.

6. A Joint Venture (JV) may submit a proposal in response to this RFP subject to the following conditions:

a. The JV is registered in the System for Award Management (SAM.gov) and has a corresponding DUNS Number.
b. The JV meets the definition of a JV for size determination purposes (FAR 19.101(7)(i)).
c. The Offeror must submit a complete copy of the JV agreement (inclusive of all JV members) that established the relationship.
d. Any member of the JV performing classified work must possess the appropriate Facility Security Clearance (FSC).

7. Official Documents and Points of Contact: The Government-wide Point-of-Entry is the Federal Business Opportunities website (https://www.fbo.gov) which is the official repository for all solicitation information related to this acquisition. All referenced documents for this RFP are available on this site. The Government is not responsible for the accuracy of information or data posted on other websites or forums. The JEDI Cloud Contracting Officer and the Contract Specialist (CS) are the **only** points of contact for this acquisition. The Offeror shall designate Authorized Personnel per Section L3.

8. Request for FOUO Documents. In order to obtain access to the For Official Use Only (FOUO) documents referenced in the Cyber Security Plan, the Offeror shall email its request and executed Attachment J-9, Company Non-Disclosure Agreement (NDA) for JEDI Cloud to the JEDI Cloud Contracting Officer, Ms. Chanda Brooks. Each company, including subcontractors, must separately execute an NDA to obtain access to the FOUO documents. Any company that receives the FOUO documents is prohibited from sharing with others; including subcontractors and teaming partners. Submissions shall be emailed to **jedi-rfp@dds.mil**, by **August 9, 2018** no later than **10:00 am ET**. The Email Subject must state: "NDA Submission". Delays will occur if the subject line varies in any manner. The FOUO documents will only be shared with companies who intend to submit a proposal, as a prime contractor or subcontractor, so the body of the email must indicate that the sender's company intends to submit a proposal in response to RFP HQ0034-18-R-0077.

9. Written Questions. Submitting **questions** via email: Any questions regarding this RFP must be submitted via email to **jedi-rfp@dds.mil** utilizing the mandatory Comment Resolution Matrix, by **August 16, 2018** at **11:00 am ET**. Verbal questions will not be answered.

10. In-Person Question and Answer. The Government intends to conduct In-Person Question and Answer (Q&A) Sessions with Offerors who plan to submit a proposal in response to the JEDI Cloud RFP. In-Person Q&A Sessions will be held at the Pentagon and strictly limited to one hour per session. Only one Q&A Session will be allotted per proposal team. If a proposing team wants an Q&A Session, the Prime Contractor (not subcontractors) shall submit a written request for a Q&A Session via email by **5:00 pm ET** on **July 31, 2018** to **jedi-rfp@dds.mil**. Requests after this deadline will not be considered. Q&A Sessions will be assigned on a first-come, first-serve basis. For complete

details about the Q&A Sessions, please see the attachment "In-Person Q&A Session Information" posted on FBO.

All participants for the Q&A Sessions must attend in person; requests for virtual attendees will be denied. Q&A Sessions are limited to a total of three Contractor personnel, one of whom must be a Principal representative from the Prime Contractor company. Attendees are prohibited from: bringing proposal or any proprietary materials to the Q&A Session; recording the session; or presenting briefs or other materials. Attendees may take notes, bring written questions, and bring portions of the RFP package about which they have questions. Further, Attendees are prohibited from bringing electronics into the meeting space. Cell phones may be stored outside of the Q&A Session space.

The purpose of these sessions is to answer Offeror questions about the RFP. Be advised that any questions regarding the feasibility of proposed technical solutions will **not** be answered.

For purposes of efficiency of the Q&A Sessions, Offerors may submit advanced written questions for Q&A Sessions via email, by **12:00 pm ET** on **August 3, 2018**, to **jedi-rfp@dds.mil**. The Government reserves the right not to answer questions in the Q&A Session and instead follow up in writing as appropriate. For example, a question may require referencing multiple documents, which may be impractical during the Q&A Session. The Government intends to release a Q&A amendment to the RFP and cautions against submitting proprietary information in any written questions.

Please note that a Government attorney may be present during each In-Person Q&A Session. Each Q&A Session will be recorded; the recording will not be provided to Offerors.

11. Proposal Submission. Submitting **proposals** via email: In order to respond to this RFP, the Offeror shall email its proposal submission to the JEDI Cloud Contracting Officer, Ms. Chanda Brooks. Submissions shall be emailed to **jedi-rfp@dds.mil**, no later than **10:00 am ET** on **September 17, 2018**. Individual email attachments cannot exceed 25 MB, and a single email cannot exceed 50 MB inclusive of attachments. Video attachments have separate submission requirements as detailed below. Multiple emails may be submitted provided that they follow the following naming conventions: The Email Subject should state: "Company Name_Email X of Y Proposal Submission for 18-R-0077." Attachment File Names shall state: "Company Name_18-R-0077_Volume X_Tab X".

Video file attachments (for Section L4, Sub-factor 1.6) must be sent via AMRDEC SAFE (https://safe.amrdec.army.mil/safe/Welcome.aspx). Offerors are strongly advised to upload video submissions at least one hour prior to the proposal submission deadline. The recipient's email address of the AMRDEC package must state **rashida.d.webb.civ@mail.mil**. Up to 25 files may be included in a single AMRDEC package, but the total submission size cannot exceed 2 GB. Offerors are encouraged to limit the number of submissions to one. In the event the Offeror requires multiple video submissions to AMRDEC SAFE, each submission shall comply with size and count restrictions as stipulated. Do not send any questions or other proposal contents to **rashida.d.webb.civ@mail.mil**, as they will not be considered or evaluated. Offerors are responsible for submitting timely proposals IAW FAR Subpart 15.208. Video Attachments shall use the following naming convention: "Company Name_18-R-0077_Video Number X of Y."

Section L2: Written Proposal Organization Instructions

1. Any pages in excess of the respective page limitations specified for each Volume/Tab, as outlined in Table L-1 below, shall not be considered during the evaluation of the proposal.

2. Page limits shall not be circumvented by including inserted text boxes/pop-ups or internet links to additional information; such inclusions are not acceptable and will not be evaluated as part

of the proposal. The Government reserves the right to verify any URLs, identified in Volume II, Tabs B, E and H, are active; the URLs will only be reviewed to validate the efficacy of the links, not the content of the website.

3. Appendices: Any items in Table L-1 identified as an Appendix are excluded from the Overall Total Page Limits for that Volume. For some Appendices, there are applicable page limits as identified in Table L-1 below. Page limits shall not be circumvented by including additional information in the appendices that is not identified in Table L-1; such inclusions are not acceptable and will not be evaluated as part of the proposal. Appendices shall be provided at the end of the respective Tab file.

4. Proposal Organization: Proposals shall consist of six separate Volumes. Initially, only four Volumes need to be submitted at the time specified in RFP Section L1 paragraph 11. Volume IV Small Business Participation Approach and Volume V Demonstration will be submitted at a later date and time. Each Tab within Volumes I through III identified below shall be submitted as separate electronic files. For Volume VI, each required MS Excel and PDF document shall be submitted as separate electronic files. All Volumes shall be organized as follows:

Table L-1

VOLUME/TAB	VOLUME/TAB TITLE	PAGE LIMIT
I	**CONTRACT DOCUMENTATION**	***Subject to Individual Page Limits Below***
TAB A	Table of Contents	No Limit
TAB B	Company Information	1 page Exclude JV Agreement and Control documentation from page count
TAB C	Cover Letter	1 page
TAB D	Signed RFP and Amendments/ Representation and Certification Information	No Limit
TAB E	EEO Pre-Award Information	No Limit
TAB F	DD Form 254 Security Classification	No Limit
TAB G	Proposal Team	No Limit
TAB H	OCI Response	No Limit

TAB I	Licenses and Service Level Agreements and Addendum	No Limit
TAB J	PWS/SOO & Factor Matrix	No Limit
TAB K	Support Contractor Proposal Access Consent Letter	No Limit
II	**FACTOR 1: GATE CRITERIA**	**Overall Total: 28 Pages**
TAB A	Sub-factor 1.1 Elastic Usage	Provide summary report as an Appendix (no page limit)
TAB B	Sub-factor 1.2 High Availability and Failover	Provide static web page document captures as an Appendix (page limit of 5 pages for paragraph 4(a) and 5 pages for paragraph 4(b)); Provide JAB documentation as an Appendix
TAB C	Sub-factor 1.3 Commerciality	
TAB D	Sub-factor 1.4 Offering Independence	
TAB E	Sub-factor 1.5 Automation	Provide static web page document captures as an Appendix (page limit of 30 pages)
TAB F	Sub-factor 1.6 Commercial Cloud Offering Marketplace	Video files submitted as prescribed in Section L1, paragraph 9; Provide catalog offering examples as an Appendix (no page limit)
TAB G	Sub-factor 1.7 Data	
III	**TECHNICAL PROPOSAL**	**Subject to Individual Page Limits Below**
TAB A	Performance Work Statement	No Limit
TAB B	Factor 2 Logical Isolation and Secure Data Transfer	30 pages for paragraphs 1-3; 3 pages per scenario in paragraph 4

TAB C	Factor 3 Tactical Edge	10 pages for paragraphs 1-2; 3 pages per scenario in paragraph 3
TAB D	Factor 4 Information Security and Access Controls	12 pages for paragraph 1; 6 pages for paragraph 2
TAB E	Factor 5 Application and Data Hosting and Portability	15 pages for paragraphs 1 and 2; 3 pages per scenario in paragraphs 3 and 4
TAB F	Factor 6 Management and TO 001	15 pages total; Provide proposed QASP as an Appendix (no page limit)
IV	**FACTOR 7: SMALL BUSINESS PARTICIPATION APPROACH** (Not included with initial proposal submission)	**No Page Limit**
V	**FACTOR 8: DEMONSTRATION** (Not included with initial proposal submission)	**No Page Limit**
VI	**FACTOR 9: PRICE**	**No Page Limit**
TAB A	Price Narrative	
TAB B	Price Information and Supporting Data for Attachment L-2 Price Scenarios	
TAB C	Price Information and Supporting Data for all CLINs	
VII	**SMALL BUSINESS SUBCONTRACTING PLAN**	**No Page Limit**

5. Each volume may contain a table of contents and glossary of all abbreviations and acronyms used that will not count towards the page limitation.

6. All pricing information shall be addressed ONLY in the Price Volume. If pricing information is included in other volumes, it will result in removal of the entire page from evaluation.

7. Format: Page size shall be 8.5 x 11 inches. Pages shall be single spaced, except for Government-provided solicitation forms or tables. At a minimum, a 12-point font size shall be used for text and a 10-point font size shall be used for any tables and/or graphics. All pages shall include page numbering and shall be numbered sequentially by volume. Volumes I, II, III, and IV of the proposal shall be submitted as a Portable Document Format (PDF) file conforming to ISO standards

32000-2, except videos. Use at least ¾ inch margins on all sides. All files shall be searchable and allow copy/paste functionality. No document or copy protections shall be used. Tables, charts, graphs, and figures shall be legible.

8. Cross-Referencing: Each volume shall be written on a stand-alone basis so that its contents may be evaluated independently. Information required for proposal evaluation that is not found in its designated volume will be deemed to have been omitted from the proposal. Unless specifically instructed otherwise in the RFP, cross-referencing within a proposal volume across Factors or Sub-Factors is not permitted. This instruction does not preclude the Government from providing proposal materials to the evaluators from different Volumes and Volume Tabs (for example, providing the PWS or Unpriced BOEs to the evaluators).

9. No classified information is required, nor shall it be provided, in any proposal. Any information marked as classified will be destroyed and not evaluated.

10. The Government will not consider alternate proposals. If an Offeror (a) fails or refuses to assent to any of the terms and conditions of this RFP, (b) proposes additional terms or conditions, (c) conditions its proposal with assumptions, or (d) fails to submit any of the information required by this RFP, the Government may consider the proposal to be unacceptable and therefore ineligible for contract award.

11. The Unpriced Basis of Estimates (BOE) requested for each of the Attachment L-2, Price Scenarios will be shared with the technical evaluators after the Government confirms the Unpriced BOE is identical, except for actual prices, to the Priced BOE.

Section L3: Volume 1 - Contract Documentation Instructions

CONTRACT DOCUMENTATION

TAB A: Table of Contents - Offerors shall include a master table of contents of the entire proposal to include each volume.

TAB B: Company Information - Offerors shall include:

Authorized Offeror Personnel. Provide the name, title, email, and telephone number of the company/division Authorized Personnel regarding decisions made with respect to your proposal and who can obligate your company contractually. Also, identify those individuals authorized to negotiate with the Government. Each of these individuals, independently, shall be authorized and empowered to make all decisions and respond to the Government in an official capacity, regardless of team formations, to include but not limited to corporate structure, team formation, or established legal entities or constructs.

Company/Division Address, Identifying Codes, and Applicable Designations. Provide company/division's street address, county and facility code; CAGE code; DUNS code; TIN; size of business (large or small). The same information must be provided for all locations that any work will be performed to support this contract.

The Offeror shall provide sufficient documentation, such as self-certification of ownership or bilaterally signed teaming/subcontracting agreements as applicable, to demonstrate control IAW Section C4 of the RFP. This documentation will be shared with the evaluators for Sub-factor 1.3 - Commerciality.

If applicable, the Offeror shall submit a complete copy of the JV agreement.

TAB C: Cover Letter - The Offeror's proposal shall include a cover letter, on the Offeror's letterhead stationery, and signed by an executive of the company with the authority to contractually bind the Offeror. The cover letter shall identify all enclosures being transmitted as part of the Offeror's proposal. The Offeror shall make a clear statement that the proposal is valid for 300 days from the proposal due date. The Offeror is required to sign and certify that all items submitted in the proposal comply with the RFP requirements.

Sample Statement of Compliance: *This Offeror hereby certifies this proposal is in compliance with the solicitation and its requirements. There are no exceptions, deviations or differences.*

TAB D: Signed Solicitation/Amendments/ Representations and Certification Information

Offerors shall provide a copy of a signed SF1449 along with any required fill-in sections within Sections B through K. The Offeror's authorized signatory shall sign the SF1449, including any amendments. Failure to submit the signed SF1449 will result in the Offeror being ineligible for award.

Section H: Special Contract Requirements. Submit Sections H2, New Services and H3, Price Changes, with the fill-ins completed.

Section I: Contract Clauses. Submit as required.

Section K: Representations, Certifications, and other Statements of Offerors. If the requested information is not available in the System for Award Management (SAM) database, submit as required.

For completion of DFARS 252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JAN 2011), the Government recognizes that this is a commercial item acquisition. For purposes of this certification, Offerors are only required to identify and assert any CDRLs in Section J Exhibit A that the Offeror is proposing to deliver with less than Unlimited Rights.

TAB E: EEO Pre-Award Information: All prime Contractors shall include in the proposal any subcontractor to which they intend to award more than $10 million IAW FAR 52.222-24, Preaward On-Site Equal Opportunity Compliance Evaluation.

TAB F: DD Form 254 Security Classification: All prime Contractors shall affirm their FSC. The Offeror shall identify the FSC for members of the JV (if applicable) and/or subcontractors. If a subcontractor also has a FSC, affirm as well.

The DD Form 254 for TO 001 will be identical to Attachment J-7 with the exception of Block 16, Certification and Signature, and Block 17, Required Distribution. The cognizant security manager for CCPO will complete Blocks 16 and 17 at contract award.

TAB G: Proposal Team: The Offeror shall provide a table listing the entire proposal team membership at all tiers. The table shall identify the company name, prime or subcontract tier of the proposed team member, and, if a team member is a wholly owned subsidiary of a parent company, name of the parent company (with clear notation that the company is a parent). The Offeror shall also provide information indicating whether they are proposing as a JV.

TAB H: OCI Response: Each Offeror shall complete the Organizational Conflict of Interest (OCI) Analysis/Disclosure Form provided in RFP Attachment L-7. If no OCI exists, then complete block 9

of the form. If any potential or actual OCI exists for this acquisition, as described in FAR Subpart 9.5, in addition to the submission of Attachment L-7, the Offeror shall submit an OCI plan with the proposal, explaining in detail how the OCI will be mitigated and/or avoided.

TAB I: Licenses and Service Level Agreements and Addendum: Each Offeror shall provide all License Agreements (whether called an End User License Agreement, Terms of Use, or some other name) and Service Level Agreements (SLAs), including third party agreements, applicable to the services that are proposed for delivery in its proposal. The Government intends to review all License Agreements and SLAs for consistency with Federal law and the Government's needs, which are reflected in the requirements in the SOO and the JEDI Cloud Cyber Security Plan and Section H1, Government Data.

The Government will accept commercial terms in a License Agreement or SLA only to the extent that those terms do not conflict with Federal law and only to the extent those terms meet the Government's needs. The Offeror shall submit the executed Addendum in RFP Section H8, Mandatory Addendum License Agreement or Service Level Agreement, as an attachment to any License Agreement(s) or SLA(s) submitted with its proposal in response to the RFP. Problematic terms beyond those in the Addendum will have to be specifically negotiated prior to award.

The Offeror acknowledges that the executed Addendum in RFP Section H8 will become a binding part of the contract and all TOs issued thereunder.

TAB J: PWS/SOO & Factor Matrix: The Offeror shall submit a cross-reference matrix using Attachment L-8, PWS/SOO & Factor Crosswalk Matrix. The PWS references shall be sufficiently specific to allow for easy identification of the task (using page, subsection, and sub-paragraph numbers as necessary). The Matrix shall address all Performance Requirements in Section 3 of the SOO, including all subsections, and any proposed Desired Capabilities in Section 4 of the SOO. Additionally, the Offeror shall map the sections of the proposed PWS to the relevant Factor(s) 2-6. The Factor mapping asserted by the Offeror does not prevent the Government from considering other PWS sections under a particular Factor that the Government deems relevant even if the Offeror did not map that PWS section to the Factor; this mapping is purely to assist evaluators in identifying the PWS section that are most likely relevant.

TAB K: Support Contractor Proposal Access Consent: The Offeror shall submit a letter clearly stating whether permission is granted allowing the contractor support identified below access to the Offeror's proposal. The Offeror and its subcontractors may choose to execute a proposal access agreement with these support contractors. Prior to the submission of a Proposal, the Offeror or its subcontractors may email **jedi-rfp@dds.mil** to obtain the point of contact information for the contractor support companies to execute any necessary proposal access agreements.

Contractor support personnel from the below listed companies under existing contracts will be used for administrative purposes only. This assistance will not include analyzing or evaluating proposals.

- Eagle Harbor Solutions
- Suntiva

Proprietary information submitted in response to this RFP will be protected from unauthorized disclosure as required by Subsection 27 of the Office of Procurement Policy Act as amended (41 U.S.C. 423) as implemented in the FAR. These companies are bound contractually by OCI and non-disclosure clauses with respect to proprietary information. Support Contractor personnel will take all necessary action to preclude unauthorized use or disclosure of an Offeror's proprietary data.

Section L4: Volume II – Gate Criteria Submission Instructions

FACTOR 1: GATE CRITERIA

The Offeror shall provide the following information for Factor 1. For purposes of this Factor and its sub-factors, Commercial Cloud Offering (CCO) means the CCO, as defined in Attachment J-8, Definitions, being proposed by the Offeror for JEDI Cloud.

Sub-factor 1.1 Elastic Usage (TAB A)

The Offeror shall demonstrate compliance with this Sub-factor by providing a summary report for the months of January 2018 and February 2018 that depicts each of the three metric areas detailed below (*i.e.*, Network, Compute, Storage). The Offeror's proposal, for all aspects of this Sub-factor, must explicitly depict CCO usage. CCO usage may include IaaS used to provide PaaS offerings, but must exclude any IaaS or PaaS usage for the CCO provider's own use including intra-company usage across different divisions or business units when those divisions or business units do not constitute separate legal entities. For this Sub-factor, CCO usage is not limited to any market segment and can include both government and non-government (public) customers.

The summary report shall include a table illustrating the addition of JEDI Cloud usage (as defined below) relative to CCO usage for the months of January 2018 and February 2018, excluding any services provided to a customer free of charge. Offerors may also include a narrative explaining how JEDI Cloud usage would not represent a majority of the three metrics areas as specified. Specifically, JEDI unclassified usage must be less than 50% of the CCO usage as demonstrated by the following:

1. Network - Volume of commercial client traffic, in bytes, for public internet ingress and egress (at the logical cloud boundary outside of availability zones, *i.e.*, in and out of the CCO-controlled infrastructure).
    a. CCO usage: aggregate of January 2018 and February 2018.
    b. For purposes of this evaluation, JEDI Cloud unclassified ingress is 10.6 Petabytes for two months.
    c. For purposes of this evaluation, JEDI Cloud unclassified egress is 6.5 Petabytes for two months.

2. Compute - Number of physical (not virtualized) compute (CPU and/or GPU) cores in use by application servers, which are defined as those physical servers that host the virtualized infrastructure and platform services used by end users (for example, a network router would not satisfy this definition of application server).
    a. CCO usage: average compute cores in use for January 2018 and February 2018 calculated by taking the sum of the total number of CPU and GPU cores in use each day between January 1st and February 28th, inclusive, and dividing it by the total number of days in that time period (average = DailyTotalsSum ÷ 59).
    b. For purposes of this evaluation, JEDI Cloud unclassified average physical compute cores in use by application servers is 46,000 cores.

3. Storage - Data, in bytes, for each of online, nearline, and offline averaged across January 2018 and February 2018.
    a. CCO usage: average storage in use for January 2018 and February 2018 calculated by taking the sum of the total storage in use each day between January 1st and February 28th, inclusive, and dividing it by the total number of days in that time period (average = DailyTotalsSum ÷ 59).
    b. For purposes of this evaluation, JEDI unclassified data storage usage averages 50 Petabytes online, 75 Petabytes nearline, and 200 Petabytes offline across the 2 months.

Sub-factor 1.2 High Availability and Failover (TAB B)

The Offeror shall demonstrate high availability and failover of the CCO data centers, defined for purposes of this Sub-factor as the physical locations containing the physical CCO hardware used to provide unclassified IaaS and PaaS services, through the following:

1. No fewer than three physical existing unclassified CCO data centers within the Customs Territory of the United States, as defined in FAR 2.101, that are all supporting at least one IaaS offering and at least one PaaS offering that are FedRAMP Moderate "Authorized" by the Joint Authorization Board (JAB) as demonstrated by documented evidence. Each data center identified must be capable of automated failover of all computing, network, and storage services to one another as demonstrated by self-certification. Geographic dispersion means that each identified data center is at least 150 miles from the others using geodesic distance as demonstrated by either a physical address or GPS coordinates for each data center;

2. Network availability through redundant and globally distributed points of presence controlled by the Offeror, as defined in Section C4 of the RFP. Globally means that there must be at least one point of presence on each continent (except Antarctica); redundant means that there are at least two or more connections providing a total bandwidth capacity of at least 40 Gigabits per second. The Offeror shall demonstrate this with a table that depicts for each point of presence: the approximate location, the number of connections to each point of presence, and the total bandwidth capacity for each connection;

3. Built-in data storage (for online, nearline, and offline) redundancy that protects against data loss in the case of catastrophic data center loss as demonstrated by a listing and description of the existing CCO offerings that provide built-in data storage as described in this paragraph for online, nearline, and offline; and

4. Provide automatic monitoring of resource utilization and events (to include failures and degradation of service) via web interface and application programming interfaces (APIs). These APIs must have online documentation that is readily discoverable as demonstrated by providing a static document capture of the web site documentation page for a and b below. Portions of documentation are acceptable. The documentation for a and b below must include example code. Each static document must include the publicly accessible URL of the source web page.
    a. Getting the resource utilization for a given virtual machine identifier; and
    b. Getting a listing of recent service health events by time and date range.

Sub-factor 1.3 Commerciality (TAB C)

The Offeror shall demonstrate the commerciality of the CCO through revenue information for calendar year 2017 in an Offeror-preferred format. The Offeror shall indicate which portion of the revenue is attributable to the CCO, the applicable company name(s) for the CCO revenue, and a breakdown of the revenue by the type of customer (*e.g.*, U.S. Federal Government versus non-U.S. Federal Government). To satisfy the commerciality of the CCO, the revenue information must show that total revenue attributable to U.S. Federal Government usage is less than 50% of total CCO revenue.

The documentation evidencing control under Section C4 that the Offeror submitted in Volume I, Contract Documentation will also be considered part of the proposal for this Sub-factor.

Sub-factor 1.4 Offering Independence (TAB D)

The Offeror shall demonstrate through a detailed narrative that the proposed solution for storage, compute, and network IaaS does not require bundling with any particular PaaS or SaaS product. Exempted from this bundling prohibition is PaaS or SaaS that is not invoiced separately and also not deployed on user provisioned cloud resources. For example, the following would not be considered bundling of IaaS with a particular PaaS or SaaS product: managed monitoring or logging services that are not-separately-priced and provided in parallel to a provisioned virtual machine by the Offeror (not through the marketplace).

Sub-factor 1.5 Automation (TAB E)

The Offeror shall demonstrate an ability to meet automation requirements for an existing API for the proposed IaaS and PaaS offerings that is capable of creating (or provisioning, as appropriate) and reading resources as identified below. This shall be demonstrated by providing a static document capture of the web site documentation page for all items listed in paragraphs 1 through 5 below. Each static document must include the publicly accessible URL of the source web page. Portions of documentation are acceptable.

1. Identity and access management:
    a. creation of an account in the JEDI Cloud;
    b. creating time-limited federated authentication tokens; and
    c. assignment of role-based access control.

2. Provisioning:
    a. creation of a single compute instances;
    b. creation of a single object storage instance;
    c. creation of a single relational database instance; and
    d. creation of a load balancing instance for virtual machines.

3. Reading of billing data:
    a. for a single account given an identifier and time and date range; and
    b. for a group of accounts as specified by the customer.

4. Reading of service usage data:
    a. usage, in hours, for all compute instances;
    b. usage, in hours, for all managed database instances; and
    c. usage, in hours, for a single compute instance based on a resource tag.

5. Security policy compliance:
    a. reading results of automated compliance scans for a single account; and
    b. reading results of automated compliance scans for a group of accounts as specified by the customer.

Sub-factor 1.6 Commercial Cloud Offering Marketplace (TAB F)

1. The Offeror shall demonstrate that the existing CCO includes an easy to use online marketplace (via web-accessible user interface) to deploy CCO and third-party platform and software service offerings onto the CCO infrastructure. The Offeror shall demonstrate the online marketplace by providing: 1) three examples of existing public catalog services for offerings for each of the categories below and 2) a narrative describing the process for end users to procure and deploy these services.
    a. Platform offerings, such as container solutions, container orchestration, code deployment, log analysis and monitoring;
    b. Advanced data analytics tools, such as machine learning, artificial intelligence, or image recognition;

c. Bring-your-own-license products for platform and software offerings from other than the CCO provider; and
d. Free and open source platform and software offerings.

2. The Offeror shall also demonstrate the CCO marketplace with two real-time, silent demonstration videos with time clock of an end user on a web interface acquiring and deploying: (1) a third-party marketplace platform offering or third-party enterprise software offering, and (2) a bring-your-own-license example from other than the CCO provider. Ease of use of self-service deployment is measured by time to launch under optimal conditions. To meet the criteria for ease of use, time to deploy must be less than 5 minutes based on the below criteria:
   a. Time starts at page-load after authentication and ends after successful deployment of the offering;
   b. Time includes entering a license if required; and
   c. Excluded from timing is the time to spin up any virtual machines to host the offering, so long as the virtual machines are required and included in the offering.

Acceptable video formats are MPEG4 and AVI.

Sub-factor 1.7 Data (TAB G)

The Offeror shall demonstrate that the proposed solution meets the following data requirements through a self-certification and with detailed technical explanations of:

1. Petabyte-scale storage and retrieval of online, nearline, and offline storage;
2. Object lifecycle management for usage based retention and data migration that operates across online, nearline, and offline storage.
3. Ability to receive the first byte from a nearline storage retrieval operation within 30 seconds as demonstrated by request and response log artifacts; and
4. Ability to retrieve 250 terabytes of arbitrary, offline storage objects within 24 hours and be accessible by applications deployed to the cloud provider's infrastructure in that time as demonstrated by request and response log artifacts.

Section L5: Volume III – Technical Criteria Submission Instructions

TECHNICAL PROPOSAL

Performance Work Statement (PWS) (TAB A)

1. Required Content for PWS: The Offeror shall provide a PWS in response to Attachment L-1, JEDI Cloud SOO. At a minimum, the Offeror's proposed PWS shall include all of the information detailed below and may be presented in the Offeror's preferred format:
   a. Detailed description of the work to be performed, including the services that the Offeror proposes to perform to achieve the SOO. The description shall be organized such that it clearly maps to the CLIN structure.
   b. Table 5.1 (verbatim) from the SOO.
   c. Table 5.2 (verbatim) from the SOO.

(end TAB A)

NOTE: For Factors 2 through 7, addressed below, the proposed PWS and any of its attachments will be considered a part of the Offeror's proposed approach. Additionally, to the extent the Offeror is proposing any desired capabilities from Section 4 of the SOO, the Offeror shall explain as part of the relevant Factor how the proposed desired capability contributes to the proposed approach for that Factor.

Factor 2 - Logical Isolation and Secure Data Transfer (TAB B)

1. The Offeror shall describe its overarching proposed approach to achieve secure data transfer using a Transfer Cross Domain Solution that is consistent with the 2018 Raise the Bar Cross Domain Solution Design and Implementation Requirements. Additionally, the Offeror shall specifically describe how the proposed Transfer Cross Domain Solution will address each of the following items:
    a. Allow an isolated enclave to transfer data to other enclaves in a highly controlled, deterministic manner, without introducing the security threats that normally come from connectivity;
    b. Provide secure one-way data transfer between logical enclaves within JEDI Cloud, to external destinations, and across classification levels;
    c. Protect enclaves from cyber threats, including malware and virus transfer, and prevent penetration by external sources;
    d. Mitigate the risk of the transfer capability as a covert channel;
    e. Enforce technical policies controlling how data transfer capabilities can be used including gaining the appropriate role-based approval for use;
    f. Allow specific role-based accounts to overrule automated security measures to securely transfer information that may be flagged as malicious;
    g. Use role-based access controls (RBAC) for the separation of administrative duties; and
    h. Local and remote monitoring, including details on how each virtual machine and tenant is monitored, how the monitoring is analyzed, and how the Offeror responds to anomalies and events.

2. The Offeror shall describe its proposed logical isolation architecture and implementation for the unclassified and classified offerings, specifically:
    a. Encryption of data at rest to include the ability for users to require the implementation of up to two layers of NSA-approved encryption utilizing algorithms and procedures specified in Committee on National Security Systems Policy (CNSSP) 15;
    b. Encryption of data in transit to include the ability for users to require the implementation of up to two layers of NSA-approved encryption utilizing algorithms and procedures specified in CNSSP 15;
    c. Logical separation with cryptographic certainty of processing between tenants within the virtualized environment to include the implementation and configuration of the hypervisor, specifically:
        i. How the virtualization system, or hypervisor, manages using a management console (MC);
        ii. How the MC communicates with its client hypervisors over a network connection that is operating at the highest security level supported by the virtualization systems;
        iii. How communications between the MC and its client hypervisors are encrypted using standards-based security protocols (*e.g.*, TLS, IPSec) using FIPS-certified cryptography;
        iv. How the hypervisor and MC shall log security and change-related events to both local and remote log repositories;
        v. How the MC operates over a secure, dedicated, and separate management network;
        vi. How the MC interface on the hypervisor is protected;
        vii. How RBAC are used for the separation of administrative duties on the MC;
        viii. How boundary protections and isolation between tenants is provided (*e.g.*,

virtual firewalls, virtual switches); and

ix. How physical and virtual intrusion detection and prevention systems shall be used to protect the hypervisor and tenants;

d. Allow for controlled cross-tenant communications, including between classification levels, via orchestrated multi-tenant peering gateways;
e. Provide users with the ability to configure secure network fabrics as needed for their applications to work and interact with each other and services outside of JEDI Cloud;
f. Local and remote monitoring, including details on how each virtual machine and tenant is monitored, how the monitoring is analyzed, and how the Offeror responds to anomalies and events;
g. Immutable logging of hypervisors and tenant activity and how immutability is achieved; and
h. Management of encryption keys by either the user or Offeror at the discretion of the user.

3. The Offeror shall describe its proposed approach to meeting the requirements for classified processing at different classification levels in accordance with section 1.3.2 in Attachment J-6: JEDI Cloud Cyber Security Plan. If logical separation is proposed between Secret and Top Secret, the Offeror shall describe the logical isolation architecture and how that architecture will meet the Section 12 Requirements for Multi-Level Security (MLS) Cross Domain Solution (CDS) in the 2018 Raise the Bar Cross Domain Solution Design and Implementation Requirements. If physical separation is proposed between Secret and Top Secret, the Offeror shall describe how they will provide a service or tool that enables users, within the constraints of enforced technical policies, to gain access to and query data at a different classification level using the Offeror's proposed transfer CDS approach with the appropriate role-based access.

4. The Offeror shall also provide a detailed description of the technical approach to Price Scenario 3(c) with a focus on how that information evidences the Offeror's secure data transfer approach.

Factor 3 - Tactical Edge (TAB C)

1. The Offeror shall describe its proposed approach to providing tactical edge compute and storage capabilities across the range of military operations that balance portability with capability. This overarching approach should not be limited to the two offerings addressed in paragraph 2 below if the Offeror is proposing tactical edge capabilities beyond the two required offerings. For each proposed tactical edge device, the Offeror shall address, at a minimum:
   a. Compute capacity capable of running multiple applications in a (a) communication degraded or disconnected environment and (b) fully connected environment;
   b. Compute capacity capable of locally running containerized applications, data analytics, and processing data;
   c. Storage capacity to retain data and files, such as but not limited to full motion video, acoustic recordings, photos, and documents, in a (a) communication degraded or disconnected environment and (b) fully connected environment;
   d. Automated bidirectional synchronization of data storage with the cloud environment at the appropriate classification level when connection is re-established. The proposed approach shall address the degree to which this synchronization order can be controlled and synchronization bandwidth use can be throttled. The proposed approach must also account for both physical (*e.g.,* wired) and remote (*e.g.,* satellite communications or over radio frequencies) connection;
   e. Quantify the electromagnetic emanations while operating in both connected and disconnected states and the ability to control the magnitude of electromagnetic emanations;

f. Ability to meet physical and logical separation requirements specified in the Attachment J-6, JEDI Cloud Cyber Security Plan;
g. High and low temperature tolerances while in storage and transit and while operating up to 100% utilization. The "Basic Hot (A2)" and "Basic Cold (C1)" daily cycles identified in Table 1, Part Three of MIL-STD-810G (page: PART THREE-10) serve as minimum storage and transit and operating temperature thresholds; and
h. The weight and physical dimensions of each proposed tactical edge device.

2. At a minimum, the proposed approach for tactical edge must include at least one offering for each of the categories below.
   a. Category One: Durable, ruggedized, and portable compute and storage. The Offeror shall describe how the offering addresses the characteristics and capabilities below.
      i. Ruggedized as defined in Attachment J-8, Definitions;
      ii. Each device should not require heavy equipment to move;
      iii. Devices may have varying compute and storage capacities along with sizes, power requirements, and physical form factors;
      iv. Industry standard input and output connectors (*e.g.*, USB-C, ethernet, and fiber);
      v. Extensible such that multiple (*e.g.*, 2, 20, 200, or 2000 units) can be connected and pool resources;
      vi. The ability to rapidly unpack, assemble, and connect the devices once they are on-site;
      vii. The ability to be powered by battery and standard military grade generators. For battery, describe the characteristics, capacity, and runtime under standby and 100% utilization;
      viii. Rapid production and supply chain processes, to include the time required to fabricate and deliver a single device and 2000 such devices; and
      ix. A mapping of the range of capability to power requirements and physical dimensions suitable for the range of military operations.
   b. Category Two: Static, modular, rapidly deployable data centers 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 OCONUS or on government owned platforms (*e.g.,* aircraft carriers, maritime operations center, airfields, and division headquarters). The Offeror shall describe how the offering addresses the characteristics and capabilities below.
      i. Rapid production and supply chain processes, to include the time required to fabricate and deliver a single data center; and
      ii. A mapping of the range of capability to power requirements and physical dimensions suitable for the range of common military operations.

In the proposal, the Offeror is cautioned to be clear and consistent with terminology and the naming conventions used for Category One and Category Two.

3. The Offeror shall also provide a detailed description of the technical approach to Price Scenario 2(a)(i-ii); Price Scenario 3(a)(i-iii); and Price Scenario 5(a)(i-ii) in Attachment L-2, Pricing Scenarios with a focus on how that information evidences the Offeror's tactical edge approach.

Factor 4 - Information Security and Access Controls (TAB D)

1. The Offeror shall provide its proposed approach for information security, specifically:
   a. Patching and vulnerability management of hardware, software, and other system components that comprise or are provided by the Offeror's proposed solution, and the ability to control enforcement of patching based on vulnerability criticality.
   b. Managing supply chain risk for hardware, software, and other system components.

c. Auditability of both the physical location and logical isolation of any hosted service to ensure compliance with security policy.
d. Automated breach identification and any processes for breach mitigation, isolation, and reporting.
e. Self-service and automated tools for preventing and remediating data spills of classified or other controlled information, including the ability to locate and erase all related data.
f. Ability to erase data and purge the associated media in both unclassified and classified environments.
g. Self-service tools to access data and analysis generated by threat detection systems. The ability to provide notifications and findings to system owners. The ability to provide raw logs to the government for analysis.
h. Ability to onboard new services into the Offeror's marketplace in a rapid and secure manner, and executing against a clearly documented process for reviewing existing marketplace offerings for security and other policy compliance. The Offeror shall provide three examples of previous new service rollouts and how each service was reviewed for security and policy compliance.

2. The Offeror shall provide its proposed approach for access controls, specifically:
a. Managing technical policies from one account to all JEDI Cloud accounts, and the ability to control access to services and restrict configuration parameters.
b. Highly granular attribute and role-based access control configuration, and the ability to assign permissions to roles IAW technical policies.
c. Object and resource access control management, including data and resource tagging.
d. Token-based and time-limited federated authentication allowing a user to assume a role within the cloud environment at all classification levels.
e. Indicate which access control capabilities are available via the Offeror's web interface, command line interface (CLI) application, and/or API.

Factor 5 - Application and Data Hosting and Portability (TAB E)

1. The Offeror shall describe its proposed approach to application and data hosting, specifically:
a. Rapid provisioning of virtual machines based on pre-defined and approved configurations stored as code either within or outside of an account, as appropriate.
b. Rapid provisioning of solitary and clustered database servers based on pre-defined and approved configurations stored as code either within or outside of an account, as appropriate.
c. Use of container-based application hosting and orchestration of multi-container deployments.
d. Hosting code functions outside of the scope of a virtual machine, typically called "serverless", which can handle both inbound network requests and can be scheduled to execute based on events.
e. Dynamic workload management software that provides automation and orchestration to elastically coordinate fluctuating workflow requests according to resource priorities, user-defined technical policies across the cloud infrastructure, or user-defined event.

2. The Offeror shall describe its proposed approach to application and data portability, specifically:
a. Exporting all data and object storage, including schemas, from one application, from multiple applications associated with a single account, and from all applications associated with all JEDI accounts regardless of storage type.
b. Exporting all system configurations, including, but not limited to, networking, routing, load balancing, and OS configuration, for a single application, multiple applications associated with a single account, and from all applications associated with all JEDI accounts.

3. The Offeror shall provide a detailed description of the technical approach to Price Scenario 1(c)(i) and Price Scenario 6(a)(i) in Attachment L-2, Pricing Scenarios with a focus on how that information evidences the Offeror's application and data hosting approach.

4. The Offeror shall provide a detailed description of the technical approach to Price Scenario 4(a)(i) and (c) in Attachment L-2, Pricing Scenarios with a focus on how that information evidences the Offeror's application and data portability approach.

Factor 6 - Management and TO 001 (TAB F)

1. The Offeror shall describe their approach to managing a program of this depth and magnitude IAW RFP Section C2 and the PWS for TO 001. The proposed approach must align with all other areas of the Offeror's proposal. The Offeror's approach to TO 001 shall include detailed processes describing how the Offeror will engage with the CCPO to achieve effective and timely communication.

2. The Offeror shall describe the process for timely remediation of issues to include, but not limited to:

   a. IaaS and PaaS performance issues
   b. Subcontractor issues
   c. Security incidents

3. The Offeror shall describe the proposed risk management process with a focus on the preemptive mitigation methods to manage risk for areas like tactical edge performance and security.

4. The Offeror shall provide the proposed Quality Assurance Surveillance Plan (QASP) for the ID/IQ. At a minimum, the QASP shall describe the approach for surveillance of contract performance and continuously meeting the performance metrics in Table 5.1 of the SOO throughout the period of performance of the contract. The Offeror shall specifically address how all required performance metrics will be assessed, analyzed and maintained through the life of the contract, inclusive of the final TO duration. Cross-referencing between the QASP and PWS is permitted, but cross-referencing between the QASP and SOO is not permitted.

5. The Offeror shall include a description of the Offeror's proposed property management system, plan, and commercial practices and standards to protect, secure, and report the GFP identified in Section F9: Government Furnished Property IAW FAR clause 52.245-1 and DFARS clause 252.211-7007.

Section L6: Volume IV – Small Business Participation Instructions

Factor 7 - Small Business Participation Approach (Only submitted per Section M2.2)

All Offerors (including prime contractors that are small businesses) shall complete Attachment J-10 Small Business Participation Commitment Document (SBPCD) and provide substantiating documentation to demonstrate how the Offeror will meet the proposed small business participation goals. This required information will be used to evaluate the extent of your commitment to use small businesses in the performance of this contract. The proposed small participation goals in Attachment J-10 will be incorporated into any resulting contract(s).

The Government's small business objective is to maximize small business participation under CLINs x003 Unclassified Cloud Support Package. For every $100,000,000 of services ordered under those CLINs, Offerors shall propose a percentage (and dollar value) that maximizes small business participation in performance of that CLIN. Prime contractors that are also small businesses may claim

credit for any services under CLINs x003 that will be performed by the prime contractor.

In addition to completing Attachment J-10, Offerors shall provide documentation evidencing the nature of the commitment with the small business concerns (SBCs) as defined in FAR Part 19 that are listed in Attachment J-10 (*e.g.*, binding letters of commitment subject only to contract award, joint ventures, mentor protégé agreements, others).

Section L7: Volume V – Demonstration Instructions

Factor 8: Demonstration (Only submitted per Section M2.2)

Offerors will be notified, at least seven calendar days prior to the Demonstration, of the date, time, and location the demonstration will take place. For planning purposes, all demonstrations will occur at or near the Pentagon. Offerors invited to provide a demonstration will be given 24-hour notice of specific scenarios to be demonstrated for evaluation purposes. All demonstrations will be recorded.

Section L8: Volume VI – Price Submission Instructions

Factor 9: Price

Offerors shall provide the following:

1. Price Overview (Tab A): The Offeror shall provide an overarching summary of its pricing proposal for overall context. Offerors are cautioned to ensure that any information submitted with its price proposal is internally consistent, consistent with the technical proposal, and consistent with the proposed catalog and RFP Section B pricing. The Offeror shall include any information in this overview necessary to support the JEDI Cloud Contracting Officer's responsibility determination under FAR Subpart 9.105.

Offerors shall submit Volume VI, Tab A, Price Narrative as a Portable Document Format (PDF) file conforming to ISO standards 32000-2.

2. Price Information and Supporting Data for Attachment L-2, Price Scenarios (Tab B): Offerors shall provide a Priced and Unpriced BOE for each of the price scenarios, and a price build-up for each of the price scenarios.

Priced and Unpriced BOE: The BOEs shall document the ground rules, assumptions, and drivers used in developing the price estimates, including applicable model inputs, rationale or justification for analogies, estimating methods, supporting schedule, and other details supporting the price estimates. The BOEs shall contain (as applicable) for each price scenario: a description of the proposed technical solution; the quantities of the applicable IaaS, PaaS, and Cloud Support offerings; an illustration of how the applicable IaaS, PaaS, and Cloud Support offerings are orchestrated together to meet the requirements of the particular price scenario; and identification of recurring and non-recurring offerings. The contents of the Priced BOE shall be consistent with that of the Unpriced BOE except that the Priced BOE shall also contain the calculations and pricing, and the Unpriced BOE shall have all pricing information removed. Offerors may use its own format for the BOEs in MS Word or MS Excel. All cell formulas shall be intact and all cells editable (*i.e.*, no locked cells). There shall be no linking to external sources.

Price Build-Up: Offerors shall provide a price build-up for the total proposed price of each scenario. The price build-up shall capture the unit prices and quantities of every item proposed for the solution. The Offeror shall use Attachment L-5, Price Scenario Price Build-up Template. All proposed pricing and methodologies for a price scenario shall be consistent with the proposed pricing for the ID/IQ,

including discount, premium, and fee methodologies. Any inconsistencies between the proposed pricing for a price scenario that deviates from the proposed pricing for the ID/IQ may render the proposal unacceptable.

Offerors are prohibited from proposing unique discount, premium, and fee methodologies that are only applicable to a particular price scenario. Offerors shall submit all price build-ups for all price scenarios as a single MS Excel workbook. The MS Excel workbook shall use formulas for all build-up calculations (*i.e.*, no manual entries) with all cell formulas intact and all cells editable (*i.e.*, no locked cells). There shall be no linking to external sources.

3. Price Information and Supporting Data for all CLINs (Tab C): Offerors shall submit separate priced catalogs for CLINs x001 Unclassified IaaS and PaaS Offerings, x002 Classified IaaS and PaaS Offerings, x003 Unclassified Cloud Support Package, and x004 Classified Cloud Support Package, for a total of four catalogs, that include a worksheet for the base period and each option period. All proposed offerings, including all proposed tactical edge and online marketplace offerings, even if any offerings are free of charge, shall be included in the applicable catalog(s). The catalogs shall include, at a minimum: Catalog Item Number; Description of Item; Item Category; the Publicly-Available Commercial Catalog Price (which is for informational purposes only); and Proposed Price for each Item. Each worksheet for option periods is limited to a narrative declaration that includes either: a) a statement that invokes the base unit pricing as of the date of the end of the previous period of performance that incorporates any price changes made pursuant to Section H2 and applies inflation or deflation rate(s) for the relevant service (either specific items, categories/groups of items, or the entire catalog), or b) a statement that invokes the base unit pricing as of the date of the end of the previous period of performance that incorporates any price changes made pursuant to Section H2. Offerors shall submit all catalogs in two versions: PDF file conforming to ISO standards 32000-2 and MS Excel workbook(s). The PDF version will be made an attachment to the contract at award. If these versions are not identical, the proposal may be deemed unawardable. No single MS Excel workbook shall exceed 25MB. All cell formulas shall be intact and all cells editable. Cell linking across workbooks is not permitted.

The Cloud Support Package catalog offerings may not be priced as time-and-materials or labor-hour as defined in the FAR Subpart 16.6. All Cloud Support Package catalog offerings shall be proposed as firm-fixed prices.

Portability Plan (CLIN x005), Portability Test (CLIN x006), and CCPO PM Support (CLIN x007) pricing shall be provided by all Offerors in the following table as part of Volume VI - Price Information and Supporting Data for all CLINs (Tab C). Offerors are cautioned to validate that the prices in the table below are identical to the proposed prices in the Section B fill-ins of the RFP. When proposing pricing for CLINs x005 and x006, the scope and complexity of the applications and data described in the Price Scenarios are illustrative examples that should inform the pricing of those CLINs, but the Government is not limited to those illustrative examples in post-award contract execution.

Table L-2

Price Component	**Unit of Issue**	**Quantity**	**Unit Price (To Be Completed by Offeror)**
Portability Plan, CLIN 0005	Each	As ordered	$
Portability Plan, CLIN 1005	Each	As ordered	$

Portability Plan, CLIN 2005	Each	As ordered	$
Portability Plan, CLIN 3005	Each	As ordered	$
Portability Test, CLIN 0006	Each	As ordered	$
Portability Test, CLIN 1006	Each	As ordered	$
Portability Test, CLIN 2006	Each	As ordered	$
Portability Test, CLIN 3006	Each	As ordered	$
CCPO Program Management Support, CLIN 0007*	Each	24	$
CCPO Program Management Support, CLIN 1007*	Each	36	$
CCPO Program Management Support, CLIN 2007*	Each	36	$
CCPO Program Management Support, CLIN 3007*	Each	24	$

*For the purpose of this CLIN, the unit of issue "EACH" equates to a month of program management services.

The Offeror shall identify all proposed discounts, premium rates, and/or fees as a separate PDF that will be made Attachment J-3, Contractor Discounts, Premiums, and Fees, to the contract at award. All terms and conditions applicable to any proposed discount and premium rates and fees (including, for example, whether it applies to specific items, categories/groups of items, or entire catalog) shall be included.

Offerors are cautioned that any proposed discounts and premium rates and fees must comply with all terms and conditions in the RFP, including, but not limited to, Sections H2, New Services and H3, Price Changes.

As noted throughout this RFP, achieving ongoing commercial parity is a key underpinning of the JEDI Cloud acquisition. This also includes ongoing parity with public commercial prices for the cloud service offerings available to DoD. Based on the anticipated volume of TOs to be issued under this ID/IQ, the Government encourages the use of most favored customer discounts.

The JEDI Cloud Contracting Officer may require additional supporting pricing data if it is determined to be necessary to reach a decision regarding the reasonableness and completeness of an Offeror's price submission. See guidance at FAR 15.403-1(c)(3).

Section L9: Volume VII - Small Business Subcontracting Plan

IAW FAR Subpart 19.7 and FAR 52.219-9, a Small Business Subcontracting Plan will be required of all Offerors, unless the prime contractor is a small business. The Small Business Subcontracting Plan shall be submitted after the determination of the competitive range when the Demonstration is conducted. Note: Attachment L-4 is provided as an instructive guideline only for the Small Business Subcontracting Plan and is not an explicit submission format requirement.

The Offeror shall provide a Small Business Subcontracting Plan to include the following information:

1. Offerors shall include a detailed approach to achieving and maintaining the small business goals throughout the life of the ID/IQ contract as established by the Offeror with its proposal in Attachment J-10, Small Business Participation Commitment Document (SBPCD).
2. Offerors shall identify all proposed subcontractors individually by name with addresses, business type (Other Than Small Business, Small Business, Small Disadvantaged Business, Women-Owned Small Business, Veteran-Owned Small Business, Service-Disabled Veteran-Owned Small Business, HUBZone Small Business, and Historically Black Colleges and Universities and Minority Institutions) as determined by the Small Business Administration size standard for the specific work being subcontracted; the principal services being provided by the subcontractor; NAICS Code; and the complexity of the services provided.
3. Offerors shall provide evidence of meeting small business goals on prior contracts. If, historically, the Offeror has not met small business goals or has never been previously required to implement a Small Business Subcontracting Plan under a Federal Government contract, an explanation shall be provided on what actions will be taken to meet the small business goals of the JEDI Cloud ID/IQ contract.
4. Offerors shall include evidence, such as binding letters of commitment subject only to contract award, of the Offeror's ability to meet the subcontracting goals.

Section L10: Solicitation Provision(s)

The following provisions are incorporated by reference:

52.204-7	System for Award Management	OCT 2016
52.204-16	Commercial and Government Entity Code Reporting	JUL 2016
52.204-18	Commercial and Government Entity Code Maintenance	JUL 2016
52.212-1	Instructions to Offerors--Commercial Items	JAN 2017
52.215-22	Limitations on Pass-Through Charges--Identification of Subcontract Effort	OCT 2009
52.225-25	Prohibition On Contracting With Entities Engaging In Certain Activities Or Transactions Relating To Iran--representation And Certifications	OCT 2015
252.239-7017	Notice of Supply Chain Risk	NOV 2013

The following provisions are incorporated by full text:

52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The Offeror is cautioned that the listed provisions may include blocks that must be completed by the Offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the Offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browsefar

https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

(End of provision)

52.252-5 AUTHORIZED DEVIATIONS IN PROVISIONS (APR 1984)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of"(DEVIATION)" after the date of the provision.

(b) The use in this solicitation of any Defense Federal Acquisition Regulation (48 CFR Chapter 2) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of provision)

252.233-9000 WHS/AD LOCAL PROVISION: AGENCY-LEVEL PROTESTS (MAR 2015)

Potential Offerors may submit an agency-level protest directly to the Contracting Officer at **jedi-rfp@dds.mil**. As an alternative to the Contracting Officer's consideration of a protest, a potential Offeror may request an independent review of their protest by a WHS Protest Deciding Official. In either case, the agency-level protest must comply with the requirements and procedures in FAR 33.103 for submitting agency-level protests. A request for an independent review by the WHS Protest Deciding Official shall be submitted to **jedi-rfp@dds.mil** and addressed to:

David Sanders, Director of WHS/AD.

The Email Subject should state: "Company Name_Agency Protest of 18-R-0077." Offerors shall direct non-agency-level protest correspondence in accordance with the instructions in Section L1, paragraphs 9 and 11.

A protest decision by the Contracting Officer or WHS Protest Deciding Official is final and not subject to appeal or reconsideration within WHS.

(end of clause)

SECTION M: EVALUATION FOR AWARD OF ID/IQ CONTRACT AND TASK ORDERS

Section M1: Basis for Award

The Government intends to award a single ID/IQ contract for JEDI Cloud to the Offeror whose proposal conforms to the RFP requirements and represents the best value to the Government, as determined by the evaluation criteria described herein, IAW the FAR. Best value will be based on a detailed evaluation of all factors outlined below. In determining the best value, the Government may employ a tradeoff process allowing for an award to other than the Offeror proposing the lowest price or achieving the highest adjectival rating.

A written notice of award or acceptance of an offer, furnished to the successful Offeror within the specified timeframe, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer, whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

When making the best value determination, only those Offerors who receive a rating of "Acceptable" for all of Factor 1 will be considered. The non-price factors, listed in descending order of importance, are as follows: Factor 2, Factor 3, Factor 4, Factor 5, Factor 8, Factor 6, and Factor 7. Non-price factors 2 through 8, when combined, are more important than Factor 9 Price. Factors 7 and 8 will only be evaluated after establishment of the competitive range. Price will become increasingly more important as the rating for each of the non-price factor ratings become increasingly equal. When the Offerors within the competitive range are considered essentially equal in terms of technical capability, or when Price is so significantly high as to diminish the value of the technical superiority to the Government, Price may become the determining factor for award.

Section M2: Evaluation Process

The Government will employ a two-phase evaluation for this acquisition.

Under Phase One, the Government will evaluate the Offeror's Volume II, Factor 1, Gate Evaluation Criteria submission, against the "Acceptable / Unacceptable" criteria identified below in Table M-2. Offerors who receive a rating of "Unacceptable" under any of the Gate Criteria Sub-factors will not be further evaluated. Thus, as an example, if an Offeror is rated as Unacceptable for Gate Criteria Sub-factor 1.2, the remainder of the proposal will not be evaluated and will not be considered for award.

Under Phase Two of the evaluation process, the Government will evaluate the Offeror's proposal using the following steps:

1. If the rating is "Acceptable" for all Sub-factors under Factor 1, Gate Evaluation Criteria, the Offeror's proposal for Factors 2 through 6 and 9 will be evaluated.
2. Upon completion of the evaluation in Phase One and Phase Two step 1, a competitive range will be established. Those Offerors in the competitive range will be invited to provide a Volume IV, Factor 7 - Small Business Participation Approach, and Volume V, Factor 8 - Demonstration, and engage in discussions (in the event the Government engages in discussions).
3. Factors 7 and 8 will be evaluated. Any Offerors for Factor 8 Demonstration that receive a rating of "Marginal" or "Unacceptable" for Technical Capability or a Risk rating of "High" shall be eliminated from the competitive range and the proposal will not be further evaluated.
4. Upon completion of discussions (if any), any Offerors remaining in the competitive range will be requested to submit a final proposal revision (FPR). The FPR shall be deemed to include the already conducted Factor 8 Demonstration.

5. The FPR will be evaluated IAW Section M. Any Offerors with a Risk Rating of "High" under any Factor shall be deemed unawardable. Any Offerors with an adjectival rating below "Acceptable" (see Tables M-3 and M-4) for any of the non-price factors (*i.e.*, Factors 2 through 8) shall not be considered for award.

6. Based on FPR evaluation, a best value determination will be made IAW Section M.

Debriefings will be conducted IAW FAR Subpart 15.5 and Class Deviation 2018-O0011, Enhanced Postaward Debriefing Rights, dated 22 March 2018.

Section M3: Evaluation Factors

Factor 1 - Gate Evaluation Criteria

Offerors' proposals will be evaluated for technical acceptability on an "Acceptable / Unacceptable" basis for each of the following sub-factors based on whether the proposal demonstrates the requirements articulated in each sub-factor IAW the respective instructions detailed above in Section L. Offerors' proposals must be rated "Acceptable" under all Factor 1 sub-factors in order to receive an overall rating of "Acceptable" for Factor 1 - Gate Evaluation Criteria. If a proposal is rated "Unacceptable" for any Gate Evaluation Criteria sub-factor, the evaluation process will immediately cease. The remainder of the proposal will not be evaluated and will not be considered for award.

Sub-factor 1.1 - Elastic Usage

The Government will evaluate whether the proposal clearly demonstrates that the addition of DoD unclassified usage will not represent a majority of all unclassified usage, per the requirements in Section L for this sub-factor.

Sub-factor 1.2 - High Availability and Failover

The Government will evaluate whether the proposal clearly demonstrates that CCO data centers are sufficiently dispersed and can continue supporting the same level of DoD usage in the case of catastrophic data center loss IAW the requirements in Section L for this sub-factor. The JEDI Cloud Contracting Officer may validate claims of the IaaS and PaaS offerings being FedRAMP Moderate "Authorized" by the JAB.

Sub-factor 1.3 - Commerciality

The Government will evaluate whether the proposal clearly demonstrates meeting the requirements of commerciality IAW Section L for this sub-factor. The Government will also evaluate if the Offeror provided sufficient documentation to demonstrate control IAW Section C4 of the RFP.

Sub-factor 1.4 - Offering Independence

The Government will evaluate whether the proposal clearly demonstrates that the proposed solution for storage, compute, and network IaaS, independent of each other, does not require bundling with any particular PaaS or SaaS product IAW the requirements in Section L for this sub-factor.

Sub-factor 1.5 - Automation

The Government will evaluate whether the proposal clearly demonstrates the ability to meet automation requirements IAW the requirements in Section L for this sub-factor.

Sub-factor 1.6 - Commercial Cloud Offering Marketplace

The Government will evaluate whether the proposal, including videos, clearly demonstrates that the CCO includes an easy to use marketplace for both Offeror native and third-party services that meets all of the requirements in Section L for this sub-factor.

Sub-factor 1.7 - Data

The Government will evaluate whether the proposal clearly demonstrates that the proposed solution meets the data requirements specified in Section L for this sub-factor.

(end Factor 1 evaluation criteria)

For Factors 2 through 7, in addition to the criteria listed below, the Government will also consider the degree to which the proposed approach and proposed ID/IQ PWS (for the sections that are applicable to the respective Factor) are consistent with each other and reflect an understanding of the Government's requirements (Section 3 and Section 5 of the SOO) as applicable to the respective Factor. The Government will also evaluate the degree to which any proposed desired capabilities from Section 4 of the JEDI Cloud SOO provide additional benefit to the Government as defined by the evaluation criteria under the respective Factor.

Factor 2 - Logical Isolation and Secure Data Transfer

1. The Government will evaluate the quality of the Offeror's proposed approach to achieving secure data transfer using a Transfer Cross Domain Solution that is consistent with the 2018 Raise the Bar Cross Domain Solution Design and Implementation Requirements. The Government will also evaluate the degree to which the proposed Transfer Cross Domain Solution will address in Section L, Factor 2(1)(a-h).
2. The Government will evaluate the quality of the Offeror's proposed logical isolation architecture and implementation for the classified and unclassified offerings and the degree to which the proposed solution will meet the requirements in Section L, Factor 2(2)(a-h).
3. The Government will evaluate the quality of the Offeror's proposed approach to meeting the requirements for classified processing at different classification levels in accordance with section 1.3.2 in Attachment 2: Cyber Security Plan.
4. For Price Scenario 3, the Government will evaluate the degree to which the technical approach and Unpriced BOE evidence a technically feasible approach when considering the secure data transfer requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenario 3 and the Offeror's overall secure data transfer approach under this Factor are consistent across the documents.

Factor 3 - Tactical Edge

1. For the proposed tactical edge devices under Section L, Factor 3(1)(a-h), the Government will evaluate how well the proposed approach balances portability against capability to enhance warfighting capacity across the range of military operations in support of national defense. The Government prefers a proposed solution that more broadly addresses the full range of military operations rather than a proposed solution that only addresses a subset of the range of military operations. The Government places far greater emphasis on existing solutions. Beyond the minimum types of devices required in Factor 3(2), the Government will consider additional capabilities that will be in production by October 14, 2019, but with lesser weight than existing solutions. The Government will also evaluate the degree to which the proposed tactical edge devices address the requirements in

Section L, Factor 3(1)(a-g) while also accounting for the practicalities of using the proposed offerings in the tactical edge environment.

2. Tactical Edge Devices for Categories One and Two

a. The Government will evaluate the degree to which the proposed approach for Category One device(s) address the requirements in items Section L, Factor 3(2)(a)(i -viii). For paragraph (2)(ix), the Government will evaluate how well the device(s) balances power requirements and physical dimensions in delivering capability within the range of military operations to forces deployed in support of a Geographic Combatant Commander or applicable training exercises.

b. The Government will evaluate the degree to which the proposed approach for Category Two device(s) address the requirements in Section L, Factor 3(2)(b)(i). For Factor 3(2)(b)(ii), the Government will evaluate how well the proposed approach Category Two device(s) balances power requirements and physical dimensions in delivering capability across the range of military operations.

3. For Price Scenarios 2, 3, and 5, the Government will evaluate the degree to which the technical approach and Unpriced BOEs evidence a technically feasible approach when considering the requirements for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenarios 2, 3, and 5, respectively, and the Offeror's overall tactical edge approach are consistent across the documents.

Factor 4 - Information Security and Access Controls

1. The Government will evaluate the quality of the Offeror's proposed information security approach and the degree to which the proposed solution meets the requirements in Section L, Factor 4(1)(a-h). As part of this evaluation, the Government will consider the following:

a. The frequency, accuracy, efficacy, and degree of automation of patching and vulnerability management of hardware, software, and other system components. The degree to which patching enforcement can be controlled based on vulnerability criticality.

b. The quality of supply chain risk management for hardware, software, and other system components.

c. The degree to which the physical location and logical isolation of hosted services is discoverable and auditable.

d. The degree to which breach identification is automated, and efficacy of processes for mitigation, isolation, and reporting.

e. The degree to which tools and automation can prevent and remediate data spills, including the efficacy of the process for locating and erasing all related data and purging all related media.

f. The degree to which the Offeror is able to erase data in any environment.

g. The degree to which data generated by all intrusion detection technology, network traffic analysis tools, or any other threat detection performed is captured. The efficacy of analysis on the data generated. The degree to which users can control the manner in which notifications are communicated, and the breadth of configuration options for alerts generated by threat detection systems. Whether the Offeror provides the ability to deliver raw logs to the Government for analysis.

h. The efficacy and quality of the process for onboarding new services into the Offeror's marketplace in a rapid and secure manner. The degree to which the Offeror was able to rapidly and securely add offerings to the marketplace in the examples provided.

2. The Government will evaluate the quality of the Offeror's proposed access control approach and the degree to which the proposed solution meets the requirements in Section L, Factor 4(2)(a-f). As part of this evaluation, the Government will consider the following:

a. The range of functionality for creating, applying, and managing technical policies for one account and across all JEDI Cloud accounts.

b. The degree of granularity of the permissions available, and the ease of discovery and assignment to roles.

c. The efficacy of the capability to tag data objects and resources for billing tracking, access control, and assignment of technical policy.

d. The range of capability, ease of implementation, and use of modern standards for federated, token-based, time-limited authentication and role assumption.

e. The degree to which the Offeror has implemented modern standards for any API and CLI access and the degree to which these APIs or CLIs, if any, match or exceed the abilities of the Offeror's web interfaces for user, account, identity, and access management.

Factor 5 - Application and Data Hosting and Portability

1. For the Offeror's proposed approach to application and data hosting, the Government will evaluate the quality of the Offeror's proposed solution and the degree to which the proposed approach meets the requirements in Section L, Factor 5(1)(a-e).

2. For the Offeror's proposed approach to application and data portability in Section L, Factor 5(2)(a-b), the Government will evaluate the following:

a. Time to execute, time to extraction, ease of use, efficacy of the mechanisms, and format interoperability when exporting all data and object storage and associated schemas for each account scenario.

b. Time to execute, time to extraction, ease of use, and format interoperability of data when exporting system configurations, including, but not limited to, networking, routing, load balancing, and OS configuration for each account scenario.

3. For Price Scenario 1 and Price Scenario 6, the Government will evaluate the degree to which the technical approach and Unpriced BOE evidence a technically feasible approach when considering the application and data hosting requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenario 1 and Price Scenario 6, respectively, and the Offeror's overall application and data hosting approach are consistent across the documents.

4. For Price Scenario 4, the Government will evaluate the degree to which the technical approach and Unpriced BOE evidence a technically feasible approach when considering the portability requirements in Section L for this Factor and the specific scenario requirements in Attachment L-2; the Government will also consider the degree to which the technical approach and Unpriced BOE for Price Scenario 4 and the Offeror's overall application and data portability approach under this Factor are consistent across the documents.

Factor 6 - Management and TO 001

1. The Government will evaluate the extent to which the Offeror's proposal evidences an effective program management approach to accomplishing the requirements detailed in RFP Section

C2 and the TO 001 PWS, and will also evaluate the likelihood that the approach will achieve effective and timely communication between the Offeror and CCPO.

2. The Government will evaluate the quality of the Offeror's proposed process for timely remediation of issues and the likelihood that issues will be timely remediated.

3. The Government will evaluate the quality of the Offeror's proposed risk management process and the likelihood that the proposed process and methods will result in preemptive mitigation for risk areas like tactical edge performance and security.

4. The Government will evaluate the likelihood that the proposed QASP will result in continuously meeting the performance metrics listed in Table 5.1 of the SOO through the life of the contract.

5. The Government will evaluate the extent to which the proposed property management system, plan, and commercial practices and standards are likely to result in protecting, securing, and reporting the identified GFP IAW FAR clause 52.245-1 and DFARS clause 252.211-7007.

Factor 7 - Small Business Participation Approach

The Government will evaluate the extent to which the proposal:

1. Section 3 in Attachment J-10, Small Business Participation Commitment Document accurately identifies the type of SBC based on the NAICS identified by the Offeror.

2. Identifies in Attachment J-10, Small Business Participation Commitment Document, the type and variety of work each SBC will perform under CLINs x003.

3. Achieves the Government's small business participation objectives for CLINs x003, Unclassified Cloud Support Package, with substantive commitments for each SBC listed in Attachment J-10, Small Business Participation Commitment Document. Offerors that propose 0% for small business participation shall be deemed Unacceptable.

Factor 8 - Demonstration

The Government will evaluate the extent to which the scenarios are successfully demonstrated using the proposed approach for Factors 1 through 6. The Government shall have access to all materials produced during demonstration as a constituent element of evaluation under Factor 8.

Factor 9 - Price

The price factor will be evaluated IAW FAR Subpart 12.209.

The Government has initially determined that adequate price competition is anticipated for this Source Selection. Certified cost or pricing data is not currently required. IAW FAR Subparts 15.403-1(b) and 15.403-3(a), other than certified cost or pricing data may be required to support a determination of price reasonableness. Certified cost or pricing data or other than certified cost or pricing data, if required to be submitted, shall be provided IAW FAR Subpart 15.403-5. If, after receipt of proposals, the Government determines that there is insufficient data available to determine price reasonableness and none of the exceptions in FAR Subpart 15.403-1 apply, the Offeror shall be required to submit additional cost or pricing data.

The Price Volume will be evaluated with respect to accuracy and completeness. This process will

involve verification that figures are correctly calculated and that proposed prices, and any applicable discounts, premiums, or fees, are accurate across the entire Price Volume. The Unpriced BOEs for each price scenario will be evaluated under the applicable Factor as specified in the Factors 2 through 5 evaluation criteria.

Task Order Price: The price for TO 001 will be evaluated to determine if it is fair and reasonable, complete, and accurate. Evaluation of options will not obligate the Government to exercise the option.

Total Evaluated Price: If there are any inconsistencies across the price proposal, or accuracy and completeness issues, that prevent the Government from identifying the proposed fixed unit prices such that the Government cannot derive the Total Evaluated Price (TEP), then the proposal may be deemed unacceptable. The Government will calculate TEP based on the following Table.

Table M-1 Total Evaluated Price

Price Component	Units	Unit Price	Total Price
Price Scenario 1 Total Proposed Price			As proposed
Price Scenario 2 Total Proposed			As proposed
Price Scenario 3 Total Proposed			As proposed
Price Scenario 4 Total Proposed			As proposed
Price Scenario 5 Total Proposed			As proposed
Price Scenario 6 Total Proposed			As proposed
Portability Plan, CLIN 0005	4 units (assuming 2 units are ordered per year for the Base Ordering Period for purposes of TEP only)	As proposed	4 Units X Unit Price = Total Price
Portability Plan, CLIN 1005	6 units (assuming 2 units are ordered per year for the Option 1 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Plan, CLIN 2005	6 units (assuming 2 units are ordered per year for the Option 2 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Plan, CLIN 3005	4 units (assuming 2 units are ordered per year for the Option 3 Ordering Period for purposes of TEP only)	As proposed	4 Units X Unit Price = Total Price
Portability Test, CLIN	4 units (assuming 2 units are ordered per	As	4 Units X Unit

0006	year for the Base Ordering Period for purposes of TEP only)	proposed	Price = Total Price
Portability Test, CLIN 1006	6 units (assuming 2 units are ordered per year for the Option 1 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Test, CLIN 2006	6 units (assuming 2 units are ordered per year for the Option 2 Ordering Period for purposes of TEP only)	As proposed	6 Units X Unit Price = Total Price
Portability Test, CLIN 3006	4 units (assuming 2 units are ordered per year for the Option 3 Ordering Period for purposes of TEP only)	As proposed	4 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 0007	24 units (assuming all months are ordered for purposes of TEP only)	As proposed	24 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 1007	36 units (assuming all months are ordered for purposes of TEP only)	As proposed	36 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 2007	36 units (assuming all months are ordered for purposes of TEP only)	As proposed	36 Units X Unit Price = Total Price
CCPO Program Management Support, CLIN 3007	24 units (assuming all months are ordered for purposes of TEP only)	As proposed	24 Units X Unit Price = Total Price
TEP			**Summation of all Total Prices**

Section M4: Technical Capability Performance Evaluation Ratings and Definitions

1. The following rating scale will be used to evaluate the Offeror's Proposal for Factor 1, Gate Evaluation Criteria (and subsequent Sub-factors):

Table M-2

Rating	Description
Acceptable	Proposal meets requirements and indicates an adequate approach and understanding of the requirements. Proposal has no strengths or deficiencies.
Unacceptable	Proposal does not meet requirements and contains one or more deficiencies and is unawardable.

2. The following adjectival rating scale will be used to evaluate the Offeror's Proposal for Factors 2 through 6, and Factor 8:

Table M-3

Adjectival Rating	Description
Outstanding	Proposal meets requirements and indicates an exceptional approach and understanding of the requirements. The proposal contains multiple strengths and no deficiencies.
Good	Proposal meets requirements and indicates a thorough approach and understanding of the requirements. Proposal contains at least one strength and no deficiencies.
Acceptable	Proposal meets requirements and indicates an adequate approach and understanding of the requirements. Proposal has no strengths or deficiencies.
Marginal	Proposal does not clearly meet requirements and has not demonstrated an adequate approach and understanding of the requirements.
Unacceptable	Proposal does not meet requirements and contains one or more deficiencies and is unawardable.

3. The following adjectival rating scale will be used to evaluate the Offeror's Proposal for Factor 7, Small Business Participation Approach:

Table M-4

Adjectival Rating	Description
Outstanding	Proposal indicates an exceptional approach and understanding of the small business objectives.
Good	Proposal indicates a thorough approach and understanding of the small business objectives.
Acceptable	Proposal indicates an adequate approach and understanding of small business objectives.
Marginal	Proposal has not demonstrated an adequate approach and understanding of the small business objectives.
Unacceptable	Proposal does not meet small business objectives.

4. The following Risk adjectival rating scale will be used to evaluate the Offeror's Proposal for Factors 2 through 6, and Factor 8:

Table M-5

Adjectival Rating	Description
Low	Proposal may contain weakness(es) which have little potential to cause disruption of schedule, increased cost or degradation of performance. Normal contractor effort and normal Government monitoring will likely be able to overcome any difficulties.
Moderate	Proposal contains a significant weakness or combination of weaknesses which may potentially cause disruption of schedule, increased cost or degradation of performance. Special contractor emphasis and close Government monitoring will likely be able to overcome difficulties.
High	Proposal contains a significant weakness or combination of weaknesses which is likely to cause significant disruption of schedule, increased cost or degradation of performance. Is unlikely to overcome the difficulties, even with special contractor emphasis and close Government monitoring.
Unacceptable	Proposal contains a material failure or a combination of significant weaknesses that increases the risk of unsuccessful performance to an unacceptable level.

Section M5: Solicitation Provision

The following provision is incorporated by reference:

52.217-5 Evaluation of Options JUL 1990

EXHIBIT D

Attachment L-1

Joint Enterprise Defense Infrastructure (JEDI) Cloud
Statement of Objectives (SOO)
As of 26 July 2018

0 Introduction

The Department of Defense's (DoD's) lack of a coordinated enterprise-level approach to cloud infrastructure and platforms prevents warfighters and leaders from making critical data-driven decisions at "mission-speed", negatively affecting outcomes. In the absence of modern services, warfighters and leaders are forced to choose between foregoing capabilities or slogging through a lengthy acquisition, rollout, and provisioning process. A fragmented and largely on-premises computing and storage solution forces the warfighter into tedious data and application management processes, compromising their ability to rapidly access, manipulate, and analyze data at the homefront and tactical edge. Most importantly, current environments are not optimized to support large, cross domain analysis using advanced capabilities such as machine learning and artificial intelligence to meet current, and future warfighting needs and requirements.

To maintain our military advantage, DoD requires an extensible and secure cloud environment that spans the homeland to the global tactical edge, as well as the ability to rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance. These foundational infrastructure and platform technologies are needed for DoD to capitalize on modern software, keep pace with commercial innovation, and make use of artificial intelligence and machine learning capabilities at scale.

This Statement of Objectives (SOO) describes the Joint Enterprise Defense Infrastructure (JEDI) Cloud acquisition of commercial infrastructure as a service (IaaS) and platform as a service (PaaS) offerings to support DoD business and mission operations. JEDI Cloud is an important first step to acquiring a general purpose cloud capable of delivering infrastructure and platform services for the bulk of the Department's mission. JEDI Cloud will also serve as a pathfinder for DoD to understand how to deploy enterprise cloud at scale while effectively accounting for security, governance, and modern architectures. This SOO is intended to maximize Offeror flexibility in proposing and delivering solutions to meet DoD's requirements.

1 Purpose

The purpose of this SOO is to describe the performance objectives, requirements, and metrics for the JEDI Cloud contract.

2 Scope

JEDI Cloud will provide enterprise-level, commercial IaaS and PaaS to support DoD business and mission operations. This means that JEDI Cloud users will include all of DoD as defined in 10 U.S.C. 111. Other potential users, subject to compliance with all applicable statutes, regulations, and policies, may include the following entities when the order is directly related to DoD business and mission operations: the U.S. Coast Guard; the Intelligence Community (excluding DoD agencies); countries with which the United States (U.S.) has collective defense arrangements as defined by the U.S. Department of State; and Federal government contractors.

JEDI Cloud services will be offered at all classification levels, across the homefront to the tactical edge, including disconnected and austere environments, and closed loop networks. JEDI Cloud services are required to meet industry-standard service level agreements (SLAs) and the requirements of this SOO regardless of where services are being delivered.

Achieving ongoing commercial parity is a key underpinning of the JEDI Cloud acquisition. To that end, there is no requirement for unclassified data center locations and network infrastructure (including points of presence and the transport layer) to be dedicated or exclusive to DoD as long as the data centers and infrastructure comply with the requirements of the JEDI Cloud Cyber Security Plan. The classified infrastructure must be physically isolated from all other Offeror infrastructure.

Unless otherwise annotated, the stated objectives, requirements, and metrics in the SOO apply across all classification levels. Also, unless otherwise stated, all date ranges in the SOO are calendar days. The Government understands that some Cloud Service Providers (CSPs) may propose functionality beyond anything specified in the SOO as part of their commercial cloud offerings. The SOO should not be interpreted as limiting any potential functionality within the proposed solution.

At a high level, there are eight primary objectives that the acquired cloud solution must achieve:

2.1. **Available and Resilient Services:** A solution that provides highly available, resilient infrastructure that is reliable, durable, and can continue to operate despite catastrophic failure of pieces of infrastructure. The infrastructure must be capable of supporting geographically dispersed users across the homefront to the tactical edge and at all classification levels, including in closed-loop networks as standalone computing and storage resources which may re-sync with global infrastructure to support warfighter operations.

2.2. **Globally Accessible:** Computing and storage resources that are securely accessible worldwide, regardless of location and connectivity status, at all classification levels. The computing and storage resources must provide assured access and enable interoperability between virtual enclaves containing applications to and data.

2.3. **Centralized Management and Distributed Control:** A solution that enables a central Cloud Computing Program Office (CCPO) to exert appropriate oversight and management of cloud services for the DoD including the ability to apply security policies; monitor security compliance and service usage across the network; and promulgate standardized service configurations; and to automate, to the extent possible, and distribute the account provisioning process, including the management of budgets and expenditures, from the CCPO to users.

2.4. **Ease of Use:** A solution that decreases the technical expertise required to effectively store data and access, deploy, and manage applications using cloud services. The solution must offer efficient self-service and initiation of computing and storage services enabling rapid development and deployment of new applications and advanced capabilities. Additionally, the solution must be capable of hosting and allowing for extraction of modern applications and structured data.

2.5. **Commercial Parity:** An environment that delivers parity with commercially available cloud service offerings where the services available to JEDI Cloud users keep pace with advancements in industry and new features are rapidly made available to JEDI Cloud users as they become commercially available. This also includes ongoing parity with public commercial prices for the cloud service offerings available to JEDI Cloud users.

2.6. **Modern and Elastic Computing, Storage and Network Infrastructure:** A solution that enables provisioning of modern computing, storage and network infrastructure that is updated and maintained regularly -- including processing architectures, servers, storage options, and platform software -- and with scale to meet consumption to enable rapid development and deployment in support of mission needs.

2.7. **Fortified Security**: Security that enables enhanced cyber defenses from the root level of systems through the application layer and down to the data layer with improved capabilities including continuous monitoring and auditing, automated threat identification, resiliency against persistent adversary threat, encryption at rest and in transit, and an operating environment that meets or exceeds DoD information security requirements.

2.8. **Advanced Data Analytics:** An environment that securely enables data-driven and timely decision making at the tactical level (within a single data domain) and strategic

level (across data domains) and supports advanced data analytics capabilities such as machine learning and artificial intelligence.

3 Performance Requirements

The requirements in this section are a minimum capability, condition, or attribute of JEDI Cloud. All time-based requirements apply to all cloud offerings, including tactical edge.

3.0 The proposed solution must be available and meet security requirements as specified in the Cyber Security Plan within 30 days of contract award for unclassified services. Classified infrastructure capable of supporting Secret services and meeting Secret-level security requirements must be provided by the Contractor within 180 days of contract award. Classified infrastructure capable of supporting all classified services (including Top Secret, SCI, and SAP) and meeting all security requirements outlined in the JEDI Form DD 254 must be provided within 270 days of contract award.

3.1 Provide computing, networking, and storage IaaS and PaaS offerings.

3.1.1 Provide a user interface for provisioning and deploying of cloud-based computing, networking, and storage services, including provisioning of pre-configured machine images, and a simple mechanism to deprovision any deployed service.

3.1.2 Provisioning a new account, user, or service offering, or deploying said offerings within JEDI Cloud, must not take any longer than the level of service that is provided in the Offeror's publicly-available Commercial Cloud assuming that the offerings have been authorized for use in JEDI Cloud.

3.1.3 The DoD must have a mechanism for activating and deactivating any cloud service offering for particular accounts or all accounts under the JEDI Cloud contract.

3.1.4 Provide a mechanism to deploy cloud-based computing and storage services based on standardized, pre-made configurations and security policies, where appropriate, and a simple mechanism to deprovision any service.

3.1.5 When an authorized user requests a cloud resource within the Offeror's portal, or via an API, the response time for when the portal confirms that resource deployment has begun must be on the order of seconds.

3.1.6 The time required to go from power off to receiving and processing user instructions (less any operating system boot time) for an individual IaaS compute instance must be on the order of seconds.

3.1.7 Provide processing unit architectures, system memory, storage capabilities, and networking options that are optimized for specific compute-based IaaS activities.

3.1.8 Provide an API Gateway service that allows JEDI Cloud users the ability to develop, deploy, secure and scale their APIs as needed.

3.1.9 Provide the ability to remotely connect to a virtual desktop environment that has access to persistent storage.

3.2 Provide the ability for JEDI Cloud to scale globally. Scalability improves computing and storage capacity, in an efficient and rapid manner, to meet mission requirements.

3.2.1 Infrastructure and networks supporting at the classified services must be physically separate from the infrastructure and networks supporting unclassified services.

3.2.2 The Offeror shall provide redundant and globally distributed points of presence available on all continents (except Antarctica) through two or more connections providing a total bandwidth capacity of at least 40 Gigabits per second.

3.3 Meet all requirements outlined in the JEDI Cloud Cyber Security Plan.

3.4 The Offeror must provide encryption and logical isolation for the unclassified and classified offerings.

3.4.1 The Offeror must provide the ability to encrypt data at rest and data in transit, such that users can choose to require the implementation of up to two layers of NSA-approved encryption using algorithms and procedures specified in Committee on National Security Systems Policy (CNSSP) 15. Users must be able to specify encryption at rest and in transit as a default configuration.

3.4.2 The Offeror must provide logical separation with cryptographic certainty of processing between tenants within the virtualized environment to include the implementation and configuration of the hypervisor.

3.4.3 Encryption keys will be managed by either the JEDI Cloud user or Offeror at the discretion of the user.

3.5 The Offeror must provide secure data transfer capability with the attributes described below.

3.5.1 Secure and highly deterministic one-way data transfer capability between logical enclaves and tenants within the cloud offering, to external destinations, including multi-tenant peering gateways, and across classification levels, while limiting any additional threats.

3.5.2 Protect enclaves from cyber threats, including malware and virus transfer, and prevent penetration by external sources.

3.5.3 Allow specific role-based accounts to overrule automated security measures to securely transfer information that may be flagged as malicious.

3.5.4 Mitigate the risk of the transfer capability as a covert channel.

3.5.5 Enforce technical policies controlling how data transfer capabilities can be used including gaining the appropriate role-based approval for use.

3.5.6 The ability to configure secure network fabrics as needed for their applications to work and interact with each other and services outside of JEDI Cloud.

3.6 The Offeror must provide automated information security and access control tools with the attributes described below.

3.6.1 Auditability of both the physical location and logical isolation of any hosted service to ensure compliance with security policy.

3.6.2 Automated breach identification.

3.6.3 Self-service and automated tools for handling data spills of classified or other controlled information.

3.6.4 Ability to erase data in both unclassified and classified environments.

3.6.5 Ability to purge data in classified environments.

3.6.6 Self-service tools to access data and analysis generated by threat detection systems.

3.6.7 The ability to provide notifications and findings of threats to system owners.

3.6.8 The ability to enable and disable services and restrict parameters within service configurations, in a manner that is easy to use by the majority of users.

3.6.9 Object and resource access control management, including data and resource tagging for billing tracking, access control, and technical policy management.

3.7 With respect to authentication, authorization, and identity and access management the Offeror must provide mechanisms for each of the below.

3.7.1 Highly granular role-based access control (RBAC) configuration within an account to include account administration, provisioning of new cloud services, and management of existing services and the ability to assign permissions to roles in accordance with technical policies.

3.7.2 Securely verify user identity using modern authentication protocols, including multi-factor authentication (MFA) and public key infrastructure (PKI) that work in all JEDI Cloud environments.

3.7.3 Federated identity support wherever the Offeror's identity management systems are in use (including across all classification levels and at the tactical edge). The Offeror must provide the ability to generate and issue time-limited, role-based authentication tokens that allow a user to assume a set of permissions within a specific account within the cloud environment.

3.8 Provide cloud-service usage and billing reports for all accounts under the JEDI Cloud contract and by specified account(s).

3.8.1 Provide a user interface to track budgets, including spend reports, cost planning and projections, and setting limits based on cloud service usage both for individual accounts and all accounts under the JEDI Cloud contract, including notifications and alerts where appropriate. Provide usage reports that contain service usage for all billable aspects offered by the Offeror. This information must be produced at the account level and for all accounts under the JEDI Cloud contract.

3.8.2 Provide an application program interface (API) with access to service usage, actual user costs, and the ability to set billing limits with notifications for individual accounts and for all accounts under the JEDI Cloud contract.

3.8.3 All billing reports and invoices must identify major categories of actual user cost drivers so that users can determine what variables are impacting consumption of the provisioned offerings and corresponding price consequences. Users must be able to set a threshold such that when spending in the specified account reaches the threshold automated notifications are sent to the user, CCPO, and Task Order Contracting Officer.

3.9 The Offeror shall provide an API for the IaaS and PaaS offerings that is capable of creating, reading, updating, and deleting resources as identified below. All areas of the API must be accessible to all JEDI Cloud users provided they have the proper access control authorization.

3.9.1 The API must provide, at a minimum, the following:

3.9.1.1 Identity and access management, including account creation and management within the JEDI Cloud contract, token-based and time-limited federated authentication, role-based access control configuration;

3.9.1.2 Provisioning and management of network configuration, compute instances, data and object storage including database management systems, and tools for scaling systems such as application server load balancing;

3.9.1.3 Storage object lifecycle management;

3.9.1.4 Reading usage data and alerts for compute, storage, and network utilization;

3.9.1.5 Reading billing data and pricing data, including by service, by specified account, and under the entire JEDI Cloud contract; and

3.9.1.6 Setting billing and usage thresholds and adding automated notifications to account owners and the CCPO.

3.9.2 The Offeror's API must be actively maintained, properly versioned, documented, and adhere to modern standards and protocols. Any changes which break backward compatibility must be announced, and JEDI Cloud users notified, at least 30 days prior to the change being put into production.

3.10 The Offeror must not bundle any offerings for storage, compute, and network IaaS, with any particular PaaS or SaaS product. For purposes of this requirement, any PaaS that uses the Offeror's infrastructure, but which is not invoiced separately and not deployed to user provisioned cloud resources, is not considered "bundled".

3.11 Generational replacement and upgrading of all hardware (compute, memory, storage, and networking) must have parity with the Offeror's publicly-available Commercial Cloud. When upgrading hardware, the new generation must have parity with the publicly-available Commercial Cloud in all cases.

3.12 Provide online, nearline, and offline storage options, as well as managed database and noSQL services at the scale and speed to meet mission requirements, including both object storage options and managed databases.

3.12.1 The Offeror must have more than one online database storage offering that can support data on the order of hundreds of Terabytes and can be queried in under one second. The offering must perform create, read, update, and delete functions on data on the order of hundreds of Terabytes within seconds, excluding network latency between the compute instance issuing the query and the database management system (DBMS).

3.12.2 The Offeror must have at least one online object storage offering that can support data on the order of Petabytes.

3.12.3 The Offeror must offer data storage solutions that include both traditional relational databases and recent alternatives in noSQL approaches such as: Key value, Graph, Document and Tuple. Versions of such database management systems must stay current with all major releases of those DBMSs.

3.12.4 There must be options for "nearline" (versus online/offline) storage solutions. Such options must provide read and write access on the order of minutes.

3.12.5 There must be options for "offline" storage solutions. Such options must provide read and write access within 24 hours.

3.13 The Offeror must have processes and rule-sets where required by the Freedom of Information Act, Federal Records Act, Disposal of Records, Executive Order (EO) 12333, EO 13587, the Privacy Act, and the Health Insurance Portability and Accountability Act, and any federal regulations implementing those policies.

3.14 Provide robust network infrastructure, suitable for handling a high volume of traffic globally, in and out of the Offeror's cloud boundary.

3.14.1 The Offeror's networking hardware, including links, network points-of-presence, and pass-throughs, must keep pace with commercially available networking hardware.

3.14.2 Network capacity, as measured by throughput and latency, must keep pace with the Offeror's publicly-available Commercial Cloud.

3.15 Provide dynamic scalability and resiliency through industry standard mechanisms.

3.15.1 The ability for users to create system configurations, either manually or through APIs, to provide automated redundancy of storage, networking and computing systems in the case of catastrophic data center loss.

3.15.2 There must be no fewer than three physical unclassified data center locations and no fewer than three physical classified data center locations within the Customs Territory of the United States, as defined in FAR 2.101. Each classification level requires at least three data centers, so if an Offeror proposes physically separate classified data centers at different

classification levels, each classification level requires at least three data centers. Each data center must be capable of automated failover of computing, network and storage services to one another within a classification level. Geographic dispersion of all data centers within a classification level is such that at least three physical data centers are at least 150 miles from each other. Unclassified and classified data centers may be co-located so long as the classified data center meets the DD Form 254 requirements.

3.15.3 Provide 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. These APIs must have online documentation that is readily discoverable, including example code.

3.16 Portability.

3.16.1 A portability plan must be provided in accordance with the Portability Plan CDRL. (CLIN x005). The portability plan must specifically identify, in the form of user instructions, the complete set of processes and procedures that are necessary to extract all online, nearline, and offline data, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a JEDI Cloud code repository, and network configurations such that any JEDI Cloud user can use these instructions to migrate from JEDI Cloud to another environment. Such procedures should be part of a consolidated, single effort versus individual export actions across separate data storage mechanisms, servers, networks, etc. within a cloud account. The portability plan must also include an explanation evidencing the ability to demonstrate successful erasing, purging or destruction of all system components, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once removed from JEDI Cloud.

3.16.2 Upon notification of the Contracting Officer, the Offeror must demonstrate portability under the Portability Test line items. (CLIN x006). The Offeror must demonstrate migration of an application and data (provided by the Government for this purpose) from JEDI Cloud to a different hosting environment. The demonstration shall validate the Portability Plan and evidence a reasonable ability to successfully migrate off of JEDI Cloud.

3.17 Provide data analytics service offerings, for example streaming analytics, predictive analytics, machine learning, and/or eventually artificial intelligence (if not currently available), available in all environments, including classified regions and disconnected environments. Such offerings must be able to operate across multiple datasets in disparate accounts across the JEDI Cloud contract.

3.18 Provide the ability to rapidly and securely deploy CSP and third-party platform and software service offerings from an online marketplace with baseline template configurations

where appropriate onto JEDI Cloud infrastructure. Software or platform offerings that cannot be deployed on JEDI Cloud infrastructure are outside the scope of this contract.

3.18.1 The online marketplace within the JEDI Cloud environment must support the ability for JEDI Cloud users to deploy CSP and third-party service offerings.

3.18.2 For third-party service offerings, the Offeror is only required to make available ones that are free, excluding the cost of IaaS resources, or where the DoD already possesses a license using the bring your own license (BYOL) approach. All free platform and software service offerings that are available in the CSP's publicly-available commercial cloud environment must also be available in the unclassified JEDI Cloud environment.

3.18.3 For BYOL, DoD will be responsible for negotiating the terms and conditions of the licenses under a separate contracting vehicle. A BYOL deployment must include integrated billing with the JEDI Cloud user's account.

3.18.4 The Offeror's marketplace must support security scanning of new and existing services being offered and also include a rapid method to notify customers using any marketplace service that a vulnerability has been discovered.

3.18.5 Deployed third-party platform and software services must include integrated billing.

3.18.6 The CCPO must be able to disable ordering of any marketplace offering for users of the JEDI Cloud contract.

3.19 Provide Tactical Edge Devices that are suitable for the full range of military operations.

3.19.1 The tactical edge computing and storage capabilities must be able to function in totally disconnected or closed loop mode, including provisioning IaaS and PaaS services, locally running containerized applications, data analytics, and processing data.

3.19.2 These capabilities must provide for automated bidirectional synchronization of data storage with the cloud environment when connection is re-established. These capabilities must also provide the ability to control synchronization order and throttle synchronization bandwidth.

3.19.3 These capabilities must also allow users to quantify and control magnitude of electromagnetic emanations.

3.19.4 The proposed solution must provide an ability to replace any tactical edge device in a manner that is suitable for the range of military operations and with minimal mission impact.

3.19.5 Upon Government request, the proposed tactical edge device shall be certified as meeting the MIL-STD-810G. The certification process is at no additional cost to the Government.

3.19.6 Tactical edge devices must include, but are not limited to, a) durable, ruggedized, and portable compute and storage, and b) static, modular, rapidly deployable data centers. To re-emphasize, the tactical edge capabilities should enable JEDI Cloud users to use cloud computing and storage resources across the range of military operations.

3.19.7 Tactical edge capabilities must follow the Cyber Security Plan, including physical and logical separation requirements, except when explicitly stated otherwise in the contract.

3.19.8 All tactical edge capabilities must be remotely configurable and maintainable to the greatest extent possible.

3.19.9 Tactical edge capabilities must support key management both on and off the device at the discretion of the user.

3.19.10 Offeror is responsible for the delivery of tactical edge devices to CONUS locations. Any services and fees associated shall be identified and priced in the relevant catalog.

3.19.11 At a minimum the operating and transporting temperature thresholds for the tactical edge devices are the "Basic Hot" and "Basic Cold" daily cycles identified in Table 1, Part Three of MIL-STD-810G (page: PART THREE-10).

3.20 The Offeror must provide prompt notification and follow up reporting on any service incidents and problems.

3.21 The Offeror must provide standard and easy-to-interpret logs, for both humans and machines, for tracking provisioning of services, configuration changes, service access and errors, and any relevant audit trail events.

3.21.1 All actions in the system, whether by a human or a machine, must be loggable to an external, non-overwritable destination also within the cloud offering. Such logs must be sufficient to provide an audit trail of activities and actions as required in accordance with DoD CIO Memorandum, Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings, dated November 15, 2017.

3.22 The Offeror must provide a pricing calculator with realistic, contractually accurate, and easy to perform price modeling and projection. The calculator must be able to make projections to support users' long-term (in excess of 12 months) planning needs.

3.22.1 Provide a range of service pricing structures that incorporate both usage-based pricing to incentivize efficient utilization of cloud computing resources and subscription models for reserved resources.

3.23 The Offeror must provide easy to understand training materials and documentation using a variety of training modalities that helps users understand how to successfully provision services and provides best practices for using services under the JEDI Cloud contract. (CDRLs A005 and A006). Separate training materials and documentation are required for tactical edge capabilities.

3.24 Provide a catalog of support under the Cloud Support Package line items in the contract to advise and assist with architecture, usage, provisioning, configuration of unclassified and classified IaaS and PaaS offerings, to include homefront to the tactical edge; and advise and assist users on optimizing the use of cloud services under the JEDI Cloud contract. Package

services shall also include training on, advising on, and assisting with integration, aggregation, orchestration, and troubleshooting of cloud services. (CDRLs A005 and A006).

3.24.1 If a Cloud Support Package offering is constrained by the number of hours available to users, then the Offeror must provide a mechanism for users to inquiry how many hours have been consumed (without that request consuming additional hours) within 24 hours of submitting a request.

3.25 Provide overarching program management capabilities under the Cloud Computing Program Office (CCPO) Program Management Support line items to oversee all contract activities for the ID/IQ during the entire period of performance of the ID/IQ. One of the purposes of CCPO Program Management Support is to align with the CCPO and provide feedback to ensure the JEDI Cloud contract is being used efficiently and in line with commercial practices. The requirements listed below are in addition to any requirements identified in any CCPO TO for CCPO PM Support.

3.25.1 Conducting any activities necessary to authorize the unclassified and classified IaaS and PaaS infrastructure and offerings.

3.25.2 Conducting continuous audit assessments and, as needed, management reviews as requested by the CCPO.

3.25.3 Providing reports for all accounts under the JEDI Cloud contract, as needed, on infrastructure hosting JEDI Cloud users' systems, including specific server hardware, network systems, power infrastructure, cooling systems, etc. and software running on those systems below the virtualization layer.

3.25.4 Delivering to the CCPO and executing the Transition Out Plan IAW Section C3: Transition Out. (CDRL A002).

3.25.5 Advising on CCPO program artifacts including acquisition life cycle documentation in an effort to maintain commercial parity.

4 Desired Capabilities

The desired capabilities are "nice to have" capabilities that are above and beyond the required performance requirements of JEDI Cloud.

4.1 Tactical Edge

4.1.1 Tactical edge capabilities that enhance warfighting advantage. For example, devices that require minimal or no external power and are capable of running for extended periods of time without battery swap or recharging. Other examples include smaller form-factor devices that are human-portable for extended periods of time; or capabilities that are deployable into air or space.
4.1.2 Innovative solutions for overcoming logistics challenges in delivering, maintaining, and/or return shipping tactical edge capabilities.

4.2 Security

4.2.1 Advanced automated security capabilities, for example, the ability to detect and respond to adversaries through artificial intelligence.

4.3 Cloud Support Package

4.3.1 Smaller, more incremental levels of support beyond the Offeror's standard Cloud Support Package offerings.
4.3.2 Includes specialized training support in various modalities, including, but not limited to, classroom, train-the-trainer, certifications, and advising on the development of training packages.

5 Performance Metrics: The metrics defined below identify the performance requirements for JEDI Cloud. These metrics will be reviewed at least annually and may change as technological advances occur.

Table 5.1*				
Item	**Objectives**	**Standard**	**Acceptable Quality Limit (must occur within time indicated within x%)**	**Monitoring Method**
1	Time to provision new VM (excludes boot time)	Under 2 minutes	95%	Activity log analysis
2	Time to spin up object storage	Under 2 minutes	98%	Activity log analysis
3	Time to spin up a 100GB block storage container and attach it to a running VM	Under 1 minute	98%	Activity log analysis
4	Response time for confirmation of job submission	Under 2 seconds	99%	Activity log analysis
5	Time required to go from power off to receiving and processing user instructions for a VM	Under 15 seconds	95%	Activity log analysis
6	Patch application and updates to underlying infrastructure and cloud services	Within 8 Hours of notification	95% of patches and updates must be completed within required time frame.	Security audit by CCPO and reporting by vendor
7	Infrastructure vulnerability disclosure to CCPO	Within 60 minutes of identification	100%. Disclosures must be identified within required time.	Security audit by CCPO and reporting by vendor

8	Alerts and notifications for budgeting and usage based thresholds	Sent within 10 minutes of crossing threshold	99%	Vendor log analysis
9	Usage metrics available in vendor API	No more than 15 minutes lag between usage and API reporting	99%	Activity log and API access
10	Actual user cost (billing) available in vendor API	No more than 24 hours lag between usage and API reporting	99%	Activity log, API access, and invoices
11	All API systems up-time	99.999 %	Uptime must be met 100% of the time.	Vendor status log analysis
12	All API response time	Less than 500 ms of added latency	98%	API and network traffic log analysis
13	Achieve classified hardware and networking commercial parity	Within 30 days from unclassified deployment (ready for IV&V testing)	100%	Report to CCPO and/or independent audit
14	Achieve classified software (DBMS, OS, Hypervisor, Hosted Services) commercial parity	Within 24 hours of unclassified deployment (ready for IV&V testing)	99%	Report to CCPO and/or independent audit
15	Time for DBMS to receive request and respond with data within single availability zone	Under 200 ms, excluding query processing time	99%	Database and network log analysis

16	Time for DBMS to receive request and respond with data across availability zones	Under 1 second, excluding query processing time	99%	Database and network log analysis
17	Offering of latest DBMS software offered as IaaS and PaaS offerings (excluding online marketplace offerings)	Less than 24 hours of public release	95%	Analysis of catalog changes over time
18	“Nearline” storage read / write the first byte	Under 30 seconds	95%	Data storage log analysis
19	“Offline” storage read / write accessible	Under 24 hours	95%	Data storage log analysis
20	Time necessary to execute plan identified in CLIN x005 is less than 12 hours	Upon notification from CO, within 12 hours to execute the demonstration	99%	Activity log analysis and/or CCPO monitoring
21	System activity logging	Less than 1 second after activity execution	99%	Activity log analysis
22	Online marketplace offering deploy time starting from authentication in the online portal	Under 5 minutes excluding time to start any infrastructure necessary to host the offering	95%	Analysis of marketplace catalog changes over time
23	Network request and response time between two VMs within the same availability zone	Under 50 ms	99%	Network traffic log analysis

24	Network request and response time between two VMs in different availability zones	Under 200 ms	99%	Network traffic log analysis
25	Make new cloud service offerings and updates and modifications to existing service offerings available in classified JEDI Cloud environment	Within 30 days (ready for IV&V testing)	99%	Report to CCPO and/or independent audit
26	Make new publicly-available commercial marketplace offerings available in classified JEDI Cloud environment (excluding any third party marketplace offerings the contract does not require to be made available to JEDI Cloud users)	Within 30 days (ready for IV&V testing)	99%	Catalog availability
27	Notification and nature of service incident impacting JEDI Cloud users	Under 10 minutes	99%	Analysis of incident reports and notifications
28	Detailed report on any service incident impacting DoD customers	Within 7 days	95%	Analysis of service incident report
29	Recovery Point Objective / Recovery Time Objective	10TB (RPO) within 5 minutes (RTO)	98%	Random Sampling
30	Delivery of portable tactical edge device in CONUS to the designated address	10 calendar days from date of order placement	80%	Random sampling

31	Delivery of modular data center in CONUS to the designated address	14 calendar days from date of order placement	80%	Random sampling

493
494 * All performance metrics apply to tactical edge capabilities unless explicitly stated otherwise.
495 For unclassified and classified tactical edge devices that are deployed, accepting any
496 modifications to the services and offerings are at the discretion of the JEDI Cloud user. If a JEDI
497 Cloud user does not accept a modification, the Offeror is not responsible for meeting
498 Performance Metrics that are directly affected by the JEDI Cloud user's decision.
499
500 **Constraints**
501
502 Any constraints are provided elsewhere in the SOO or listed in the Cyber Security Plan.
503
504 **Deliverables**
505

Table 5.2

CDRL	Deliverable	Frequency / Date of First Submission	Medium/Format/# of Copies	Submit To
A001	Contract Monthly Progress Report	Monthly	Electronic copy in Offeror's preferred format	CCPO
A002	Transition Out Plan	As required	Electronic copy in Offeror's preferred format	CCPO
A003	Contract Security Management Plan	Within 30 days of contract award and then annually thereafter; updated annually or as required to reflect necessary changes.	Electronic copy in Offeror's preferred format	CCPO

A004	Technology Refresh Plan	Within 30 days after contract award and then semi-annually thereafter	Electronic copy in Offeror's preferred format	CCPO
A005	System Administrator Training Materials	Within 30 days after award; updated annually or as required	Various	CCPO and Ordering Activity
A006	Role-Based User Training Materials	Within 30 days after award; updated as required	Various	CCPO and Ordering Activity
A007	Portability Plan	Within 60 days of contract award	Electronic copy in Offeror's preferred format	CCPO
A008	Contract Ordering Guide	Within 15 days after Government developed sections provided; updated annually or as required to reflect necessary changes.	Electronic copy in Offeror's preferred format	CCPO
A009	Change Management Roadmap	Within 90 days of contract award, then annually thereafter	Electronic copy in Offeror's preferred format	CCPO
A010	Quality Control Plan	Within 30 days of contract award, then annually thereafter	Electronic copy in Offeror's preferred format	CCPO

A011	Security Authorization Package	Various depending classification level	Electronic copy in format acceptable to the FedRAMP process	CCPO
A012	Technical Report	As required	Electronic copy in Offeror's preferred format	CCPO
A013	Small Business Reporting	Annually after date of contract award	Electronic copy in Offeror's preferred format	CCPO
A014	Portability Test	As required	In accordance with the Portability Plan	CCPO
A015	Task Order Monthly Progress Report	As required	Electronic copy in Offeror's preferred format	CCPO and/or Ordering Activity
A016	Meeting Materials	Quarterly	Electronic copy in Offeror's preferred format	CCPO

Unless otherwise specified, the Government shall have fifteen calendar days to review and provide comments to all deliverables. Any deliverables that are not commented upon within that time frame are deemed approved. Offeror shall have five calendar days to revise and resubmit any deliverables that the Government provides comments upon.

EXHIBIT E

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1336	Draft SOO	2	2 5	3	83	How can Commercial Cloud providers comply with DOD security requirements?	Accreditation requirements are outlined in the draft Cyber Security Plan updated in draft RFP #2.
1337	Draft SOO	2	2.7	3	97	"Fortified Security" is not a DOD specification	The intended meaning of Fortified Security, for purposes of JEDI Cloud, is defined in section 2.7 in the draft SOO.
1338	Draft SOO	3	3	3	118	DOD Security Requirements cannot be met in the time frames identified. If this requirement stays only AWS and Microsoft can bid,	There is no requirement for Offerors to have accredited classified environments at the time of proposal. The SOO requires the proposed solution to be available and meet the requirements as specified in the Cyber Security Plan within 30 days of contract award for unclassified services; within 6 months of contract award for classified services at the Secret level; and within 9 months of contract award for classified services at the Top Secret/Sensitive Compartmented Information (TS/SCI) and Special Access Program (SAP) levels.
1339	Draft SOO	3	3	4	122	Cloud Solution Providers do not deliver at the tactical edge. The requirement needs to discuss the desired outcome not a "prescriptive" solution	The draft SOO released with draft RFP #2 provides the performance objectives, performance requirements, and performance metrics relevant to the tactical edge requirements.
1340	Draft SOO	3	3 2	4	129	Cloud boundary is a undefined term. The Government needs to clarify what that means to DoD.	"Cloud boundary" is defined in Attachment 8 Definitions of draft RFP #2.
1341	Draft SOO	3	3 3	4	135	JEDI cloud regions are undefined. Is the government seeking an Industry solution or prescribing one?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1342	Draft SOO	3	3 6	4	144	Please define "CCPO"	The CCPO is the Cloud Computing Program Office. This office works directly for the Chief Management Officer and will manage the JEDI Cloud, as was explained in the JEDI Cloud Q-A Matrix for draft RFP #1. For example, reference ID #54.
1343	Draft SOO	3	3 9	4	156	Will PKI and MFA replace CAC identity management?	The JEDI contractor must provide MFA via DoD PKI (CAC), non-DoD PKI, and other industry standard authentication methods as further detailed in the Cyber Security Plan.
1344	Draft SOO	3	3.1	4	157	DoD needs to define the "specific DOD Organizations" that will be requiring usage reports	The usage and billing reporting requirements have been updated to be by account, group of specified accounts, or all accounts associated with JEDI Cloud.
1345	Draft SOO	3	3.1.6	5	3878	Would the Government provide and example of "third party Platform and software service"?	A cloud marketplace is an online storefront, operated by a cloud provider, to which customers may subscribe to PaaS and SaaS offerings that run on the cloud provider's infrastructure. The specific third party PaaS and SaaS marketplace offerings are dependent upon the particular cloud provider. SaaS and PaaS offerings that cannot be deployed on the JEDI Cloud are outside of the scope of this acquisition.
1346	Draft SOO	3	3.2.2	5	199	The requirement is not clear	There is no section 3 2 2 in the draft SOO. The Government is unclear as to the meaning of this question.
1347	Draft SOO	4	4.1	6	214	How does the JEDI Cloud Security Plan incorporate the DOD Cloud Security guide?	Accreditation requirements are outlined in the draft Cyber Security Plan as updated in draft RFP #2. The incorporation of the DoD Cloud Computing Security Requirements Guide, and the applicable exceptions, are addressed in the draft Cyber Security Plan.
1348	Draft SOO	4	4.7	6	236	How can the Government dictate a percentage of utilization to a CSP. The nature of the environment is such that this is not practical.	The requirement to maintain a certain level of utilization will be removed for the final RFP, but regular reporting about utilization levels will remain.
1349	Draft SOO	4	4.7	6	236	Does the 50% criteria extend to the tactical edge? Or is it an all encompassing measurement?	The requirement to maintain a certain level of utilization will be removed in the final RFP, but regular reporting about utilization levels will remain. The requirement will be clarified in the final RFP.
1350	Draft SOO	4	4 8	7	241	How will DoD Measure the evergreen infrastructure of the CSP? How will Security controls be applied?	The Government is unclear as to the meaning of this question.
1351	Draft SOO	4	4.14	7	3290	How is "nearline" storage defined. Do you have a use case for it?	"Nearline" storage is defined in Attachment 8 Definitions of draft RFP #2.
1352	Draft SOO	4	4.19	8	3920	Can the Government provide a description or example of the "portability" requirement?	The scope of work required for the Portability CLINs are described in Section 4 of the draft SOO with RFP #2.
1353	Draft SOO	4	4.2.9	9	364	How does this requirement map to a CSP model? The CSP is responsible for the Cloud Content. This is prescriptive.	The purpose of this requirement is to ensure that JEDI Cloud maintains ongoing commercial parity with the cloud vendor's publicly-available offerings. There are performance metrics in the SOO that also address commercial parity requirements.
1354	Draft SOO	9	4.2.8	9	331	Is the transition plan for the entire DOD cloud or would it be for "tenants"? The requirement is not clear.	The Transition plan is for the enterprise and the portability plans address the "tenants." Clarification will be provided in the final RFP.
1355	Draft RFP Section H	H	H-7	19	345-362	This clause reads a default for a cyber attack. It is too restrictive in the DOD environment.	This clause allows the Government to terminate without cure notice if failure to meet security requirements is due to the Contractor's willful misconduct. It is reasonable for the Government to expect contractors to not engage in willful misconduct.
1356	Draft RFP Section H	H	H-13	21	457-471	Terms of conflicting License need to be addressed. The Government requested a BYO-License offering in the PWW. How will conflicting terms be handled?	With Bring Your Own License, the Government would have negotiated the terms of the license agreement under a separate contracting vehicle. The Section H clause entitled "Third Party Marketplace Offerings" addresses the fact that the JEDI Cloud contractor is not responsible for BYOL licensing terms.
1357	Draft RFP Section L	L	L-9	91		Small business requirements are not applicable to this procurement. Imposing them on the CSP's will only drive the Governments cost up.	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation.
1358	Draft SOO	3	3 2	4	131	Why is this an objective versus a design concept?	The Statement of Objectives is framed in terms of performance objectives, performance requirements, and performance metrics.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1359	Draft SOO	4	22	8	309-324	CLIN 4 talks about the portability plan for data, yet with the emphasis on AI and Machine Learning, how is the government going to address moving those AI and ML-based services and associated capabilities? For example, if I use AI/ML services in CSP #1, and then want to move to CSP #2, I can transfer all my data over using CLIN 4 procedures, but all the specifics of the AI/ML services can be proprietary to the CSP so how does the government intend to move those services over?	The Government recognizes that not all features of a specific Offeror's cloud environment will be portable should the Government decide to move to a different hosting environment for a particular application and/or data.
1360	Draft SOO	3	1	4	125	For OCONUS non-tactical support, will the government be providing data center space to the CSPs, or is the CSP expected to leverage OCONUS contractor-owned facilities via foreign subsidiaries?	There are two types of OCONUS requirements. The first is OCONUS tactical edge capabilities, and the static, modular, rapidly deployable data centers are required to be on military controlled locations. The second is the points of presence requirements. Per the Cyber Security Plan, all infrastructure, excluding networking equipment and points of presence, must be within US customs territory or on US military installations.
1361	General	Factor 1	1.7	87		Aside from the timed demos, how will the government evaluate/score the requirement for an on-line marketplace? Is there a minimum number of 3rd party offerings? Minimum # of native CSP-to-3rd party integrations? Any other criteria aside from what is listed?	The Government's evaluation criteria are provided in Section L and M.
1362	Draft SOO	2	2.4	2	78	t is clear that the government realizes apps need to be either modern or re-engineered to move into the JEDI cloud. How does the government intend to determine which legacy apps will be re-engineered, and for those that can't/won't be re-engineered, what is the government's intent for those apps?	The Government is aware that some applications may require modernization. System owners are responsible for architecting and optimizing applications and data that they migrate to the JEDI Cloud.
1363	Draft SOO	3	3.4	4	132	Scalability and resiliency as currently deployed and enabled in cloud providers does not follow an industry standard paradigm, i.e.,. the APIs and services for resiliency that CSP #1 provides are not transferable to CSP #2 without re-architecting each application being moved. All CSPs implement these services in a proprietary nature unique to their specific platform. Has the government considered including off-boarding/re-architecting services for these services in CLIN 4? As it reads now, CL N 4 is dedicated solely to data transfer, but has not considered application and/or service/API re-platforming issues.	Transition and migration services are outside the scope of this contract.
1364	Draft SOO	3	3.21	5	195	(Also related to draft pricing scenario #2-ERP). The proposed scenario focuses on the size of the ERP system's database, and lists requests per minute for performance. A) Would the government consider pricing these database services at the single server level, i e., provision a database server and pay for actual consumption of compute (CPU/Memory) resources over time as traffic varies, instead of on a reserved basis? This would be a combination of the usage-based and reservation-based pricing models. b) If so, how would the government compare this methodology to the two methods listed in SOO 3.21. c) Has the government considered requiring performance-based SLAs for these databases? Typically, ERP systems must have a dedicated database instance, and need guaranteed levels of performance to meet application response time requirements.	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1365	General				98	Will the government provide guidance on the mandated use of existing DoD security architecture (i.e. JRSS, Service component gateways, base level TLA stacks, Cloud Access Points, etc.) if alternative security solutions are acceptable, what cyber security data/reporting is required? Will the government provide additional guidance on the required use of existing Cyber Security Service Providers and the relationship and reporting to service component (Army/Navy/AF/USMC) Cyber Component Headquarters	The Cyber Security Plan sets forward the security requirements that must be met.
1366	Draft SOO	3		3	118	What specific changes to the existing C&A process (i e.. DISA's review & oversight) are proposed to allow CSPs to meet these delivery timelines? The current, mandated processes will not allow anyone to meet these objectives.	Department policy decisions are outside of the scope of the draft solicitiation. The Cyber Security Plan sets forward the security requirements that must be met.
1367	Draft SOO	3	3 2	4	131	Will the government require the use of existing DISN infrastructure to include Cloud Access Points to connect customers to this new cloud service? If not, will connection criteria be provided to identify authorized connection solutions and will certification/Authority to Connect procedures be required for these new DoD network connections?	The Draft Cyber Security Plan in draft RFP #2 states that the Contractor is required to establish direct fiber links to DoD Meet-Me-Points for unclassified connections.
1368	Draft SOO				147	Will the government mandate the use of existing (CAC based) authentication methods and infrastructure (i.e., PKI) to access new cloud services? If no, how will new multi-factor authentication solutions be evaluated by security officials?	The JEDI contractor must provide MFA via DoD PKI (CAC), non-DoD PKI, and other industry standard authentication methods.
1369	Draft SOO				235	Can the government explain the intent of the requirement that the CSP provider not exceed 50% of public capacity?	The requirement to maintain a certain level of utilization will be removed in the final RFP, but regular reporting about utilization levels will remain. The requirement will be clarified in the final RFP.
1370	Draft SOO	4	4.27		356	Will the government be prepared to identify and deliver existing/owned licensing to be leveraged within the marketplace?	The responsibilities for licensing terms and conditions for third party offerings in the marketplace are clarified in clause H-15 in draft RFP #2.
1371	Draft CyberSec Plan	4	4.1.4	4	135	Will facilities (floor space, power, cooling, etc.) and base/facility access be provided to the CSP for overseas locations to adequately support the tactical warfighter environment from US controlled bases/installations? If so, how will the government manage/charge for this facility use/access?	The Government, not the JEDI Cloud contractor, is responsible for establishing the appropriate facilities to support tactical edge capabilities.
1372	Draft CyberSec Plan	4	4.4.5	6	173	Will the governments 'meet me points' mirror or requirement include existing DISN Cloud Access Points (CAPS)? If so, what bandwidth/real throughput to customers will be guaranteed to the existing base level networks?	The Government intends to access the Contractor's cloud services via both the meet-me-points and the Internet. The Government is responsible for providing adequate access and throughput from the DISN to the meet-me-points and Internet.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1373	Draft SOO	Cost table	Cloud Support Package	6	58	Migration services are key to the success of JEDI and need to be available to the Government. Affixed price or hourly rates should be included and mapped to the SOW requirements	Transition and migration services are outside the scope of this contract.
1374	Draft RFP Section C	C1	Performance works statement	14	132	Migration services will be key to the success of JEDI. The Government should describe the "migration vision" in the PWS.	Transition and migration services are outside the scope of this contract.
1375	Draft PWS Template	C2	c-3, b, vi	14	154	The Government is seeking accreditation without a commitment to Industry. If Industry accredits the solutions how will the Government guarantee usage?	Usage is not guaranteed beyond the stated ID/IQ contract minimum.
1376	Draft RFP Section C	C4	b	15	183	This reads as the Government will be entering into "an oral contract"	Depending on the urgency, the initial direction may be made orally, but the final RFP will clarify that the direction will be reduced to writing as soon as practicable.
1377	Draft RFP Section C	F3	n/a	16	225	The Government must identify locations for service as to ensure response, availability, and support.	Your comment has been noted.
1378	Draft RFP Section C	H4	SOFA	17	277	Non-Federal entities do not know what SOFA is or how to comply.	The Status of Forces Agreement clause has been removed from Section H in the final RFP.
1379	Draft RFP Section C	H5	a. - New services	18	288	How can New Services be proposed with the limitations stipulated by the Government in the SOW.	There is nothing in the SOO that prohibits incorporation of new services so long as it complies with all contract requirements.
1380	Draft RFP Section C	H5	c- Price Premium	18	303	Too prescriptive (i e. percentage of increase for new services).	The Section H clause for new serices has been updated to balance the requirement for commercial parity with Offeror pricing flexibility.
1381	Draft RFP Section C	H-13	License Agreement or terms of use	21	455	Not clear as to who is responsible for the agreements	The Offeror is responsible for all agreement with the exception of Bring Your Own License offerings.
1382	Draft RFP Section C	H-13	Assignment by Licensor	25	n/a	The government must accept license terms to have consistency in SLA's and terms.	The Government is prohibited from accepting terms that are inconsistent with Federal laws.
1383	Draft RFP Section C	H-14	third party market place offerings	27	529	Will the Government define the scope of "bring your own license"? Vague at best.	Based on market research, Bring Your Own License is a common offering for cloud provider marketplaces.
1384	Draft RFP Section C	I	Availability of funds	29	561	Funding must cover the period of performance and not started and stopped each Fiscal Year.	Your comment has been noted.
1385	Draft RFP Section L	Tab C	Tactical Edge	85	n/a	The 19 page total is confusing. With 10 and 3 per scenario. What does the Government want to see? Is pricing or a narrative required or both?	For the tactical edge evaluation criteria, the Offeror is allocated 10 pages to address the elements outside of the Pricing Scenarios. For the invoked Pricing Scenarios, the Offeror is required to provide a technical approach to each invoked Pricing Scenario; the Offeror is limited to 3 pages per Pricing Scenario.
1386	Draft RFP Section J	Attachment 4	5c Multiple data uplink options to include fiber optic, low and high bandwidth Ethernet, and compatibility with standard sitcom systems			Do the uplink options need to be routed through the Container?	The Government is unclear as to the meaning of this question. However, any tactical edge device must be able to accept connections through a Government provided uplink.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1387	Draft RFP Section J	Attachment 4	5c Multiple data uplink options to include fiber optic, low and high bandwidth Ethernet, and compatibility with standard sitcom systems			Will the sitcom systems reside in the Container	The Government is unclear as to the meaning of this question. However, any tactical edge device must be able to accept connections through a Government provided satellite uplink.
1388	Draft RFP Section J	Attachment 4	5c Multiple data uplink options to include fiber optic, low and high bandwidth Ethernet, and compatibility with standard sitcom systems			will there be a requirement for the sitcom antenna's or any other antenna's require mounting on the Container?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1393	Draft RFP Section C					How is the Government evaluating the "Tactical Edge" support plan? There does not seem to be any mention of it in sections L or M. How will the Prime provide support. Will the requirement be on-site?	The manner in which DoD intends to evaluate tactical edge is described in Sections L and M. The requirements for support to the tactical edge are described in the SOO.
1394	Draft SOO	2	2.7	3	107-111	To enable root level system security, it is imperative that the DoD maintain ownership and separation of the data keys, while encrypting the data prior to entering the cloud environment. Does the JEDI program require DoD agencies to maintain a root level of trust through key ownership and separation as well as data encryption?	Encryption keys will be managed by either the government or Offeror at the discretion of the user. The requirements for cryptographic certainty have been been clarified in the Cyber Security Plan with the final RFP.
1395	Draft SOO	3	3 5	4	139	Monitoring and auditing service security should be made possible through an additional layer of security, outside of the cloud environment, prior to entering the cloud.	Your comment has been noted.
1396	Draft CyberSec Plan	1	1.1.2	1	27	In the interest of data protection, security and privacy, we highly recommend the DoD require all JEDI CSP personnel and contractors to be US Citizens.	Your comment has been noted.
1397	Draft CyberSec Plan	4	4.4.1	3	111	Requiring crytographic certainty of encryption is important, however this addresses only half of the data security equation. The keys to encrypt and decrypt the data must be owned by the DoD and must reside outside of the Cloud in a key management system. A key management system is available as hardware or a software solution and provide a root of trust, owned by the DoD.	The final Cyber Security Plan has been updated to clarify the Government's requirements.
1398	Draft SOO	3	3 8	4	151	Does DoD expect the PKI mechanism used to address this requirement to be the same an existing PKI infrastructures used in DoD (CAC cards, SIPR cards, etc) or are you looking for new PKI infrastructure for identities assigned to system administrator, as other agencies are doing. If new identities, must these share space on existing tokens and cards (ie. use of multi-identity cards or multi-purpose tokens) or will new cards or tokens be required?	The JEDI contractor must provide MFA via DoD PKI (CAC), non-DoD PKI, and other industry standard authentication methods.
1399	Draft SOO	3	3 9	4	154	Does the government see the possibility of Out-of-Band identify solutions, such as one time passwords, as a viable mechanism to meet this federated identity requirement?	Any federated identity solution must include time-limited, role-based authentication tokens. While one time passwords may be part of that solution, it does not alone meet the requirement.
1400	Draft SOO	2	2.7	3	110	Can the government provide any specific information security requirements that would be required for the encryption of data at rest and in transit? For example, would NIST SP 800-53 govern the data at rest and the data in transit operating environment?	The Offeror must encrypt data at rest and data in transit to include the ability for users to require the implementation of up to two layers of commercial grade encryption utilizing algorithms and procedures specified in Committee on National Security Systems Policy (CNSSP) 15.
1401	Draft SOO	4	4.32	10	376-382	Given the requirement for an abiliytn to operate at the tactical endge in disconnected mode with all containerized applications, one implicit assumption is that all keys necessary for application usage at the tactical edge must be resident on the edge device. Does the government requirements a specific F PS 140-2 key protection level for keys resident on the tactical edge. Is a F PS 140-2 level 2 or 3 requirement to be imposed, or will software only key protection (FIPS 140-2 level 1) be allowed for storage of highly sensitive keys?	The final SOO has been clarified to state that tactical edge capabilities must support key management both on and off the device at the discretion of the user. The classification level involved and expected connection status will likley drive this decision.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1402	Draft SOO	4	4.34	10	394	Must encryption and logical isolation of classified and unclassified data be provided within a single edge computing environment, or is it acceptable to meet this objective with a separate set of tactical endge computing environments?	The tactical edge devices must comply with the physical and logical isolation requirements for classified information. The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1403	Draft SOO	4	4.34.1	10	396-399	If two layers of commercial encryption are required, it is also a requirement that those solutions be provided by separate encryption vendors?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1404	Draft SOO	4	4.35.1	11	408	Per existing DoD policy, transfer of data across isolated enclaves and especially across classification levels requires a UCSDMO approved cross-domain solution (CDS), which typically requires being run on a dedicated hardware platform with a hardened OS. Is the JEDI team proposing virtualized CDS solutions now be deployed on a virtualized cloud infrastructure, with or without approval from UCDSMO, or is the JEDI team expecting offerers to provide UCDSMO approved CDS hardware devices in the data centers hosting these cloud services (and potentially comingled with commercial cloud offerings)?	The secure data transfer requirements have been clarified in the evaluation criteria and Cyber Security Plan. The Government does not intend to provide the Contractor a particular cross domain solution; the Contractor is required to provide a secure data transfer capability in accordance with the Cyber Security Plan and SOO. The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1405	Draft SOO	4	4.35.2	11	411	Will the data transfer capability described here provide the government with the ability to create newDoD policies that govern the data transfer between enclaves based on such characteristics as file type, data volume, QoS and others? How does content checking play into this paradigm?	The draft SOO provided with draft RFP #2 included a requirement that the data transfer capability be able to enforce technical policies controlling how data transfer capabilities can be used.
1406	Draft SOO	4	4.35.7	11	421	An orchestrated multi-tenant peering gateway is not an industry standard term with a known set of requirements. How does the JEDI team see this component being evaluated for completeness and efficacy. Must it meet all requirements of a cross domain solution, a subset of those requirements, or a new set of requirements. If the latter, do any of those requirements address content inspection, which is not directly addressed in this DRFP, and if so, is it incumbent upon the offerer to specifiy what rerquirements its orchestrated multi-tenant peering gateway will meet, or will the government provide more specific requirements in future iteratrions	The SOO with the final RFP has been updated to clarify these requirements. The term orchestrated multi-tenant peering gateway is no longer used.
1407	Draft SOO	4	4.34.1	10	396	Will there be a requirement to encrypt data traversing commercial carriers' circuits.	The Offeror must encrypt data at rest and data in transit to include the ability for users to require the implementation of up to two layers of commercial grade encryption utilizing algorithms and procedures specified in Committee on National Security Systems Policy (CNSSP) 15.
1408	Draft CyberSec Plan	1	1.1	3	71-72	All references to Impact Levels have been removed from this draft. However, Section 1.1 of this document states: "1.1 The Contractor is responsible for following the DoD Cloud Computing Security Requirement Guidelines,". By including this requirement to meet the DoD Cloud Computing Security Requirement Guidelines, bidders will be required to achieve L5 and IL6 certification to be in compliance. If the goal is to remove Impact Level certifications, clear exceptions should be added to this section. If impact level certifications are required, please add explicit requirements directly back within this document to clearly outline the impact levels and deadlines required.	While the Cyber Security Plan invokes the DoD Cloud Computing Security Requirements Guide, the Cyber Security Plan also established certain deviations from the CC SRG. The Cyber Security Plan does not require prior accreditation.
1409	Draft CyberSec Plan	C	C.3 and C.4	10	270-272	All references to Impact Levels have been removed from this draft. However, Section 1.1 of this document states: "1.1 The Contractor is responsible for following the DoD Cloud Computing Security Requirement Guidelines,". By including this requirement to meet the DoD Cloud Computing Security Requirement Guidelines, bidders will be required to achieve L5 and IL6 certification to be in compliance. If the goal is to remove Impact Level certifications, clear exceptions should be added to this section. If impact level certifications are required, please add explicit requirements directly back within this document to clearly outline the impact levels and deadlines required.	While the Cyber Security Plan invokes the DoD Cloud Computing Security Requirements Guide, the Cyber Security Plan also established certain deviations from the CC SRG. The Cyber Security Plan does not require prior accreditation or certification.
1410	Draft SOO	5	Table 5.1	14	Row 13	This requirement states that: "Classified software (DBMS, OS, Hypervisor, Hosted Services) parity" [must be achieved in] "Less than 24 hours from unclassified deployment". This 24 hour requirement will effectively require that bidding CSPs install and configure software for all new services within the classified environment and harden them to be ready for FedRAMP High Certification days to weeks or even months ahead of deployment in the unclassified/commercial environment. This requirement will force the awarded CSP to deploy all new services into the classified environment first regardless of its applicability to the DoD mission. It will also delay a CSP from being able to deploy services to its commercial/unclassified marketplace which will limit its ability to capture return on development investments. This requirement should be extended to allow time for services to be deployed, configured and hardened within the classified environment only after they have been successfully deployed and adopted by customers in the commercial/unclassified domain. Adequate time should also be provided for these services to be fully installed, configured, and hardened within the classified environment. Depending on the scale and scope of these future services the time to do so could be significant.	The requirement has been clarified to state "Within 24 hours of unclassified deployment (ready for IV&V testing)."

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1411	Draft SOO	5	Table 5.1	16	Row 25	The requirement to make marketplace offerings available in the classified environment within 30 days cannot be enforced by most or all CSPs. The business decision of whether to invest the CapEx and OpEx needed to offer a service in the JEDI classified environment's marketplace ultimately lies with the 3rd party marketplace vendors. Similarly the deployment time cannot be controlled by the hosting CSP. Recommend removing this requirement as it cannot be practically met by any bidders.	The requirement has been clarified to state "Within 30 days (ready for IV&V testing)."
1412	Draft SOO	4	4	6	206-210	In the latest draft, the timeline still states that unclassified workloads must be "available and meet accreditation and authorization requirements within 30 days of contract award for unclassified services." The cyber security plan indicates that the requirement for unclassified workloads is FedRAMP moderate. Question: Given that FedRAMP certification timelines are highly dependent on the work of the FedRAMP assessment team (JAB, etc.). Will the DoD allow bids that include services that are deemed FedRAMP ready within 30 days of award, with the understanding that they cannot be sold within the JEDI cloud until FedRAMP moderate accreditation is met? We sincerely hope that you will consider this requirements enhancement, as doing so will help bidders to maximize the breadth and depth of their JEDI catalog of services, and will ensure that new services are available as soon as possible after award. We believe that allowing this change is in the spirit of the cloud acceleration goals of their contract.	While the Cyber Security Plan invokes the DoD Cloud Computing Security Requirements Guide, the Cyber Security Plan also established certain deviations from the CC SRG. The Cyber Security Plan does not require prior accreditation or certification. The Gate Criteria for Sub-factor 1.2 - High Availability and Failover has also clarified the applicable FedRAMP requirements.
1413	Draft SOO	4	4	6	206-210	In the latest draft, the timeline still states that classified workloads must be available and meet accreditation and authorization requirements within 6 months of contract award for classified services at the secret level. The cyber security plan indicates that the requirement for classified workloads is FedRAMP High. Question: Given that FedRAMP High certification timelines are highly dependent on the work of the FedRAMP assessment team (JAB, etc.). Will the DoD allow bids that include classified secret services that are deemed FedRAMP ready within 30 days of award, with the understanding that they cannot be sold within the classified secret environment within the JEDI cloud until FedRAMP High accreditation is met? We sincerely hope that you will consider this requirements enhancement, as doing so will help bidders to maximize the breadth and depth of their JEDI catalog of services, and will ensure that new services are available as soon as possible after award. We believe that allowing this change is in the spirit of the cloud acceleration goals of their contract.	While the Cyber Security Plan invokes the DoD Cloud Computing Security Requirements Guide, the Cyber Security Plan also established certain deviations from the CC SRG. The Cyber Security Plan does not require prior accreditation or certification. The Gate Criteria for Sub-factor 1.2 - High Availability and Failover has also clarified the applicable FedRAMP requirements. The Cyber Security Plan has clarified the federal and DoD policies applicable classified infrastructure.
1414	Draft SOO	4	4	6	206-210	In the latest draft, the timeline still states that classified workloads must be available and meet accreditation and authorization requirements within 9 months of contract award for classified services at the top secret level. The cyber security plan does not explicitly provide requirements for classified workloads at the Top Secret level, but indicates generally that the requirement for classified workloads is FedRAMP High. Question: Can you confirm that there are no additional accreditation requirements beyond FedRAMP High for Top Secret workloads or update the RFP to include those requirements.	While the Cyber Security Plan invokes the DoD Cloud Computing Security Requirements Guide, the Cyber Security Plan also established certain deviations from the CC SRG. The Cyber Security Plan does not require prior accreditation or certification. The Gate Criteria for Sub-factor 1.2 - High Availability and Failover has also clarified the applicable FedRAMP requirements. The Cyber Security Plan has clarified the federal and DoD policies applicable classified infrastructure.
1415	Draft SOO	4	4	6	206-210	In the latest draft, the timeline still states that classified workloads must be available and meet accreditation and authorization requirements within 9 months of contract award for classified services at the top secret level. The cyber security plan does not explicitly provide requirements for classified workloads at the Top Secret level, but indicates generally that the requirement for classified workloads is FedRAMP High. Question: Given that FedRAMP High certification timelines are highly dependent on the work of the FedRAMP assessment team (JAB, etc.) and that Top Secret accreditation requirements have not yet been provided, will the DoD allow bids that include classified top secret services that are deemed FedRAMP ready within 30 days of award with the understanding that they cannot be sold within the classified secret environment within the JEDI cloud until FedRAMP High accreditation and to-be-defined Top Secret accreditation are granted? We sincerely hope that you will consider this requirements enhancement, as doing so will help bidders to maximize the breadth and depth of their JEDI catalog of services, and will ensure that new services are available as soon as possible after award. We believe that allowing this change is in the spirit of the cloud acceleration goals of their contract.	While the Cyber Security Plan invokes the DoD Cloud Computing Security Requirements Guide, the Cyber Security Plan also established certain deviations from the CC SRG. The Cyber Security Plan does not require prior accreditation or certification. The Gate Criteria for Sub-factor 1.2 - High Availability and Failover has also clarified the applicable FedRAMP requirements. The Cyber Security Plan has clarified the federal and DoD policies applicable classified infrastructure.
1416	General	0	0	0	0	There were numerous questions submitted in response to the first draft RFP asking whether the Government requirement is for one cloud service provider providing one cloud or open to multi-cloud teaming arrangements. In response to those questions, the Government has repeated over and over the same answer stating, "Offerors may propose any kind of teaming/partnering arrangement so long as the proposed solution meets the requirements of the solicitation." But what is the "requirement"? That is the question.	Offerors may propose any kind of teaming/partnering arrangement so long as the proposed solution meets the requirements of the solicitation. The requirement is everything in the RFP package.
1417	General	0	0	0	0	Please state – yes or no – is the Government's JEDI requirement for one cloud?	JEDI Cloud is a single award ID/IQ contract for commercial IaaS and PaaS at all classification levels.
1418	General	0	0	0	0	Is a multi-cloud solution – 2 or more CSPs working together – acceptable assuming it otherwise meets the SOO of the RFP?	Offerors may propose any kind of teaming/partnering arrangement so long as the proposed solution meets the requirements of the solictiation.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1419	General	0	0	0	0	Leading industry analyst IDC states in its worldwide cloud predictions for 2017 that by 2018, "[o]ver 85% of enterprises will commit to multicloud architectures encompassing a mix of public cloud services, private clouds, community clouds, and hosted clouds" and that "[b]y the end of 2018, more than 50% of enterprise-class businesses will subscribe to more than five different public cloud services and will continually add, expand, contract, and drop subscriptions based on business needs." t further explains that "Dispersed 'hybrid cloud' and 'multicloud' IT environments will be the rule" and that businesses as a result should "[m]aster the integration and management of hybrid cloud and multicloud environments," which will be "a fundamental requirement for operating." The various reasons for this trend include the importance of tailoring particular workloads to the cloud solution for which they are best adapted, the ability to take advantage of new and innovative services from all providers (not just a single provider), and the ability to secure the best price and take advantage of new pricing and service models. What is DOD's assessment of this report in the context of the JEDI cloud initiative?	DoD is not going to use the solicitation process to provide feedback on a third-party report.
1420	General	0	0	0	0	For indefinite-delivery, indefinite-quantity contracts with broadly defined scopes of work, the law strongly favors awarding multiple contracts so that the government can benefit from competition as specific task orders are articulated in the future. The more ill-defined the scope of work, the greater the need for competition at the task order level. How will DOD meet this requirement given the broadly defined JEDI scope of work?	Your comment has been noted.
1421	General	0	0	0	0	If the government intends to migrate applications, how will the government assess the various IaaS and PaaS offerors' ability to enable the performance of existing or newly built applications in their clouds?	Transition and migration services are outside the scope of this contract.
1422	General	0	0	0	0	If this RFP is meant to be complementary to other cloud service contracts, even within DoD, what is the government's justification for making a single award in this procurement?	While not required by acquisition law, the DoD's rationale for single award has been published with the final RFP.
1423	General	0	0	0	0	Is there a requirement for any of the services at the higher classification level to be delivered inclusive of support solely from a government controlled environment?	The cloud support package requirements have been clarified in the SOO with the final RFP.
1424	General	0	0	0	0	The government did not specifiy the number of ICD705 compliant datacenters to meet the Top Secret, SCI, and SAP requirements in the RFP. Will two ICD 705 compliant datacenters separated by the same distances as the unclassified datacenters be acceptable?	The SOO has been updated to require at least 3 classified data centers.
1425	Draft CyberSec Plan	1	1.1.0	3	74	Please give more details on logical separation requirements for and between Commercial, L2, L4, IL5, does this allow separate Virtual Machine on Same Server?	If the Offeror is able to ensure logical separation with cryptographic certainty at the processor and storage levels between VMs on the same server, this would be allowed. Physical separation at the processor level along with cryptographic certainty to address storage isolation is also acceptable.
1426	Draft CyberSec Plan	1	1.1.0	3	74	Please give more details as to where the Cryptographic Certainty should be applied in logical separation?	Cryptographic certainly should be applied such that there is no inadvertant communication or traffic transferred between logically separated workloads. The Department is looking for vendors to provide innovative products and services while following industry standards and best practices.
1427	Draft CyberSec Plan	1	1.1.0	3	74	Can a Commercial Non-DoD Virtual Machine be on the same Server as L5 DoD virtual as long as it is logically separated with cryptographic certainty?	If the Offeror is able to ensure logical separation with cryptographic certainty at the processor and storage levels between VMs on the same server, this would be allowed. Physical separation at the processor level along with cryptographic certainty to address storage isolation is also acceptable.
1428	Draft CyberSec Plan	3	0	4	108	This states that the offeror must meet requirements at or beyond commercial capabilities. Since the CSP Offeror is based on a commercial capability, and the CSP Offeror already does R&D to advance new technology for their commercial cloud offerings, will the government fund the CSP to invent this technology that goes beyond what is currently being developed and also provide the requirements for such unforseen new inventions?	DoD will not separately fund the vendor's R&D activities under the JEDI Cloud contract.
1429	Draft CyberSec Plan	4	1	4	118	This specifies at least 3 data centers. How will the government provide survivability of DoD's IT enterprise if easy to identify and disable data center facilities were taken out by foreign or domestic bad actors, and wouldn't the government want multiple clouds providers with a vast number of data centers to avoid a risk of national defense survivability?	Your comment has been noted.
1430	Draft CyberSec Plan	4	3	5	155	Can the government specify the list of future hardware vulnerabilities that will arise so the offeror can meet this requirement? If not available, suggest rewriting requirement to hardware that is hardened but upgradeable if vulnerabilites arise.	This requirement has been clarified in the Cyber Security Plan with the final RFP.
1431	Draft CyberSec Plan	4	4	4	113	How much of a goegraphic distance is required for the data centers for Secret, Top Secret Top Secret/Sensitive Compartmented Information (TS/SCI), Special Access Program (SAP) levels?	The SOO has been clarified to require at least 150 miles apart for data centers at different classification levels.
1432	Draft CyberSec Plan	4	4.01	4	118	Are 3 Data Centers for HA needed for Unclassified workloads(L2, IL4, L5)?	The approved Cyber Security Plan has been updated to clarify the Government's requirements.
1433	Draft CyberSec Plan	4	4.01	4	118	Are 3 Data Centers for HA needed for Secret, Top Secret Top Secret/Sensitive Compartmented Information (TS/SCI) and Special Access Program (SAP) levels?	The approved Cyber Security Plan has been updated to clarify the Government's requirements.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1434	Draft CyberSec Plan	4	4.4	5	161	What are the networking separation requirements for the data center in separating internet traffic coming into data center for (Commercial or IL2 systems) and for NIPR NET Coming in Via DoD CAP to L4/IL5 systems?	The Department would like the ability for applications within logical enclaves to be accessible from the internet, from NIPRNet, or from both at the discretion of the appropriate Authorizing Official. Traffic should be separated by the Offeror so that systems not authorized for internet access do not have internet traffic. The DoD is looking for vendors to provide innovative products and services while following industry standards and best practices.
1435	Draft RFP Section C	C	1	14	132	If migration services are outside the scope of the procurement, how will DoD assess the total cost of moving to a single cloud service provider?	Transition and migration services are outside the scope of this contract. The Department is not going to comment on other contracts outside the scope of JEDI Cloud as part of this RFP process.
1436	Draft RFP Section F	2	2	16	221	Section F2 states that orders with 5 option years can be awarded and option years can be exercised after the expiration of the JEDI contract. Can the term of the marketplace be extended by a task order with option years extending beyond the expiration of the JEDI contract?	This language has been clarified in the final RFP. Task order option years cannot be exercised after the expiration of the JEDI Cloud contract.
1437	Draft RFP Section H	2	0	17	257	DoD should prohibit the JEDI contractor from using Government data, aggregating Government data or data mining for its commercial purposes.	Your comment has been noted.
1438	Draft RFP Section H	3	C	17	275	With this statement will the conntractor be responsible for all cryptographic devices being supplied to support connectivity for the program?	The government will utilize multiple mechanisms for cryptographic certainty, including those provided by the Offeror.
1439	Draft RFP Section H	14	c	27	540	How will a dispute between a Third Party Offeror and the IaaS provider be resolved?	The specific circumstances and facts would drive the path to resolution.
1440	Draft RFP Section H	14	c	27	540	DoD should ensure there is no requirement imposed by the JEDI contractor for vendors to list or sell products through the JEDI contractor's commercial marketplace as a condition for selling through the JEDI marketplace.	The marketplace requirements are addressed in the SOO and Section H of the RFP.
1441	Draft RFP Section M	3	Factor 3	102	3923	What is the rationale for the RFP's preference of "existing solutions" at the Tactical Edge?	Unclassified tactical edge offerings must be available within 30 days of contract award.
1442	Draft RFP Section M	4	Factor 10	106	4079	How will price reasonableness be evaluated for sales through the marketplace?	The online marketplace requirements have been updated to restrict the types of offerings that are required. Price reasonableness for online marketplace will be evaluated in accordance with Section M, which has been updated for clarity.
1443	Draft SOO	0	0	1	11	The SOO states that the goal of the RFP is to modernize the currently fragmented systems in order to allow for information sharing and greater data analysis. Would DoD consider making multiple awards and requiring cloud service providers to ensure interoperability, particularly if this cloud service contract is meant to be complementary?	The requirement remains as stated.
1444	Draft SOO	2	0	2	43	Will "international allies and partners" be able to submit tasks orders directly to the JEDI contractor?	This language has been clarified in the final RFP. The SOO scope is intended to permit the possibility of international allies placing orders, but there are a multitude of statutory and regulatory considerations that DoD would have to resolve before any such orders could be placed.
1445	Draft SOO	2	0	2	43	What is the statutory/regulatory authority that allows "international allies and partners" to order directly from the JEDI contractor?	The SOO scope is intended to permit the possibility of international allies placing orders, but there are a multitude of statutory and regulatory considerations that DoD would have to resolve before any such orders could be placed.
1446	Draft SOO	2	0	2	43	Who are the "international allies"?	This language has been clarified in the final RFP.
1447	Draft SOO	2	0	2	43	Who are the "partners"?	This language has been clarified in the final RFP.
1448	Draft SOO	2	0	2	43	Will International allies and partners be permitted to purchase tactical edge services?	The SOO scope is intended to permit the possibility of international allies placing orders, but there are a multitude of statutory and regulatory considerations that DoD would have to resolve before any such orders could be placed.
1449	Draft SOO	2	0	2	43	How will DOD handle export law and ITAR requirements for orders by "international allies and partners"?	The SOO scope is intended to permit the possibility of international allies placing orders, but there are a multitude of statutory and regulatory considerations that DoD would have to resolve before any such orders could be placed.
1450	Draft SOO	2	0	2	43	Will these orders by "international allies and partners" be handled as FMS sales?	The SOO scope is intended to permit the possibility of international allies placing orders, but there are a multitude of statutory and regulatory considerations that DoD would have to resolve before any such orders could be placed.
1451	Draft SOO	4	4.26	9	348	Since offerors will likely propose a broad range of different third-party vendors, how will purchases of third-party vendor offerings through the online marketplace meet the CICA requirements for competition?	The JEDI Cloud contract will be awarded pursuant to full and open competition.
1452	Draft SOO	5	0	13	448	What is the basis of the performance metrics identified in Table 5.1? Are they derived from actual mission requirements or based on the performance of a particular Cloud Service Provider?	The performance metrics reflect DoD's requirements for JEDI Cloud.
1453	Draft RFP Section L	L6	Factor 8 - Small Business SubK Plan	97	3681	Factor 8 references the total value of CL Ns x00401 and x00501; is this a typographical error? We did not find these CLIN's listed however CL N's x00104 Cloud Support Package and x000105 Portability Plan are possibly the intended reference.	This has been corrected in the final RFP.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1455	Draft RFP Section L	Section L4: Volume II	Sub-factor 1.2 High Availability and Failover	90	3310	Would the government please provide further clarity in the definition of points of presence.	Points of presence has been added to Attachment 8 Definitions with the final RFP.
1456	Draft RFP Section L	Section L4: Volume II	Sub-factor 1.1 Elastic Usage	88-89	3261-3282	Does the Government intend all network traffic from the Offeror's commercial cloud infrastructure supporting JEDI to flow through a DoD boundary cloud access point?	The Draft Cyber Security Plan in draft RFP #2 states that the Contractor is required to establish direct fiber links to DoD Meet-Me-Points for unclassified connections.
1457	Draft RFP Section L	Section L4: Volume II	Sub-factor 1.1 Elastic Usage	88-89	3283-3294	Please provide expected utilization for Secret and Top Secret similarly to the compute and storage numbers given for Unclassified.	Sub-factor 1.1 will only be evaluated for unclassified usage.
1458	Draft RFP Section L	Section L4: Volume II	Sub-factor 1.1 Elastic Usage	88	3263	Please delete the word "Revenue" from line 3263 as the revenue requirement has moved to sub-factor 1.3- Commerciality.	The referenced instance of the word "revenue" has been removed in the final RFP.
1459	Draft RFP Section L	L5 Volume III	Factor 7	97	3669	Given the Government is asking for basis of estimates on more than 12 different systems and environments, please confirm the basis of estimates information is excluded from page count.	The BOEs are excluded from the page counts.
1460	Draft SOO	5	Table 5.2	17-18	459-460	Will the Government please provide definitions of examples or templates of the deliverables in table 5 2 of SOO	The CDRLs describe the requirements for deliverables.
1461	Draft SOO	2 and 3	4.23	9	326-335	Please confirm that DoD intends the Offeror to provide commercially available cloud services that are hosted in its "Unclassified Infrastructure" in OCONUS locations to be constructed on DoD-provided US customs territory or military installations (within the Customs Territory of the United States, as defined in as defined in FAR 2.101); and that this "Unclassified Infrastructure" will not be required to be dedicated for exclusive DoD use. Foreign commercial customers and foreign Government organizations may consume commercial cloud services hosted on DoD-provided US customs territory or military installations in OCONUS locations.	The requirements in the Cyber Security Plan are for services (unclassified and classified) to be provided from data centers located within the Customs Territory of the United States. Services will be provided OCONUS through redundant and globally distributed points of presence controlled by the Offeror and available on all continents (except Antarctica). The Department will use a combination of tactical edge devices, such as static, modular, rapidly deployable data centers, as specified in the SOO to enable dedicated services OCONUS without relying on connectivity. These tactical edge devices must be dedicated and not used/accessed by other customers.
1462	Draft CyberSec Plan	4	4.1.2 and 4.1.4	4 and 5	131 and 135	Please confirm that DoD intends the Offeror to provide commercially available cloud services that are hosted in its "Unclassified Infrastructure" in OCONUS locations to be constructed on DoD provided US customs territory or military installations (within the Customs Territory of the United States, as defined in as defined in FAR 2.101); and that this "Unclassified Infrastructure" will not be required to be dedicated for exclusive DoD use. Foreign commercial customers and foreign Government organizations may consume commercial cloud services hosted on DoD provided US customs territory or military installations in OCONUS locations.	The requirements in the Cyber Security Plan are for services (unclassified and classified) to be provided from data centers located within the Customs Territory of the United States. Services will be provided OCONUS through redundant and globally distributed points of presence controlled by the Offeror and available on all continents (except Antarctica). The Department will use a combination of tactical edge devices and static, modular, rapidly deployable data centers as specified in the SOO to enable dedicated services OCONUS without relying on connectivity. These tactical edge devices must be dedicated and not used/accessed by other customers.
1463	Draft RFP Section L	L6: Volume IV	Factor 8 Small Business Subcontracting Plan	97	3681	Please clarify the CL Ns that the Small Business Participation and Subcontracting Plan apply to as the text identifies CLINs x00401 and x00501. Does the requirement apply to CLINs 103 and 104?	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation, which only applies to the Unclassified Cloud Support Package CLINs.
1464	Draft PWS Template	Task Order 002	3.0 Performance Requirements	6	265	Under which CL N does the Government expect the Offeror to provide a 24x7 tier 1 help desk?	The Government would generally expect help desk support to be offered under the Cloud Support Package CLINs.
1465	Draft RFP Section L	M2 and M4	1 and 2	100 and 107	3819-3821 and 4103-4104	Section M2.1 states under step two that the Offeror's proposal for Factors 2 through 7 and 10 will be evaluated in accordance with section M adjectival ratings. Section M4.2 states the following adjectival rating scale will be used to evaluate the Offeror's Proposal for Factors 2 through 7 and Factor 9. Please change Factor 10 to Factor 9 in line 3820 or provide further clarity that is more consistent between M2 and M4.	This language has been corrected in the final RFP.
1466	Draft RFP Section L	Section L6: Volume IV	Factor 8 Small Business Subcontracting Plan	98	3706-3708	With regard to the following requirement: The Offeror shall provide a Small Business Subcontracting Plan to include the following information: 3. Offerors shall provide evidence of meeting small business goals on prior contracts. If, historically, the Offeror has not met small business goals, an explanation shall be provided on what actions will be taken to meet the small business goals of the JEDI Cloud ID/IQ contract. Will a copy of an Offeror's most recent Summary Subcontract Report, which includes a "Remarks" section, filed as required by an approved commercial plan as defined by FAR 19.701 meet this requirement? If not, will a separate description of the actions that will be taken by the Offeror to meet the small business goals of the JEDI Cloud ID/IQ contract meet this requirement?	The small business participation approach, which is now Factor 7 in the final RFP, no longer requires evidence of historical achievements of meeting small business goals. This Factor also now uses an adjectival rating scheme.
1467	Draft RFP Section L	Section L5: Volume III	Factor 3 Tactical Edge (Tab C) ii.2	94	3536-3537	Please define "compute capacity" as either traditional VM style processing (IaaS) or both traditional (IaaS) and modern micro-computing style processing (PaaS) (e g. containers, functional compute, etc.)	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1468	Draft RFP Section L	Section L5: Volume III	Factor 3 Tactical Edge (Tab C) ii.4	94	3541-3544	Does "physical" refer to wired networking? And, does "remote" refer to wireless LoS and SATCOM networking?	Factor 3 has been clarified in the final RFP.
1469	Draft RFP Section L	Section L5: Volume III	Factor 3 Tactical Edge (Tab C) iii.1.b	95	3554	Please confirm that "not require heavy equipment to move" refers to MIL-STD-1472G, page 202, 5.8.6.2.5 Portability.	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1471	Draft RFP Section L	Section L4: Volume II	Sub-factor 1.4 Offering Independence	90	3345-3349	Are monitoring solutions to get telemetry about the offers environment considered PaaS for the purpose of this factor?	This requirement has been clarified in the final RFP.
1472	Draft RFP Section L	Section L4: Volume II	Sub-factor 1.4 Offering Independence	90	3345-3349	Is a cloud HSM (key management) used to manage keys for encrypting the IaaS data store considered PaaS for the purpose of this factor?	This requirement has been clarified in the final RFP.
1473	Draft RFP Section L	Section L5: Volume III	Factor 2 Logical Isolation and Secure Data Transfer (TAB B) item i (2)	93	3494	Can the Offeror assume that "implementation of up to two layers of commercial grade encryption" refers to the use of a dual VPN tunnels (e g. a tunnel inside a tunnel), encrypting twice with two different keys, for encryption in transit?	Dual VPN tunnels would be one method for implementing two layers of encryption; however, the Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1474	Draft RFP Section L	Section L5: Volume III	Factor 2 Logical Isolation and Secure Data Transfer (TAB B) item iii (7)	94	3517-3518	Can the Offeror assume "between classification domains" refers to controlled cross-tenant communications between networks at different classification levels (e.g. communication between SECRET and TOP SECRET//SCI)?	The language in Section L has been updated to "classification levels" in the final RFP.
1475	Draft RFP Section L	Section L5: Volume III	Factor 2 Logical Isolation and Secure Data Transfer (TAB B) item iii (7)	94	3517-3518	Do controlled cross tenant communications require compliance with CNSS Policy 12, which states "The cognizant AO, in coordination with the System and Information Owner, and the Unified Cross Domain Services Management Office (UCDSMO) must validate requirements and proposed solutions for interconnecting security domains containing data of different classification or releasability for applicable systems, in accordance with CNSSI No. 1253 Appendix-F Attachment-3 (CNSSI No. 1253F3), Cross Domain Solution Overlay"?	The security requirements are addressed in the Cyber Security Plan.
1476	Draft RFP Section L	Section L5: Volume III	Factor 2 Logical Isolation and Secure Data Transfer (TAB B) item iii (2)	94	3508-3509	Will the Government please define what "information levels" are?	The language in Section L has been updated to remove this reference in the final RFP.
1477	Draft RFP Section L	Section L5: Volume III	Factor 2 Logical Isolation and Secure Data Transfer (TAB B) item iii (7)	94	3517-3518	Will the Government please define what "orchestrated multi-tenant peering gateways" are?	This term has been removed in the final RFP.
1506	Draft CyberSec Plan	4 Requirements	4.0 Geographic	4	115	To support geographic redundancy, as well as OCONUS operations, may cloud providers offer services to the DoD in OCONUS Datacenters/Regions located within FVEYs or NATO member nations?	The requirements in the Cyber Security Plan are for services (unclassified and classified) to be provided from data centers located within the Customs Territory of the United States. Services will be provided OCONUS through redundant and globally distributed points of presence controlled by the Offeror and available on all continents (except Antarctica). The Department will use a combination of tactical edge devices and static, modular, rapidly deployable data centers as specified in the SOO to enable dedicated services OCONUS without relying on connectivity. These tactical edge devices must be dedicated and not used/accessed by other customers.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1507	Draft RFP Section L	Section L5: Volume III	Factor 3 (Tactical Edge)	95	3558	Will the Government further describe the capability desired in the statement '...such that 2, 20, 200, or 2000 units can be connected and pool resources"?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1508	Draft RFP Section L	Section L5: Volume III	Factor 3 (Tactical Edge)	95	3553	In regards to MIL-STD-810G, the majority of the tests are tailored in accordance with artifacts like the Life Cycle Environmental Profile (LCEP). In lieu of not having such a document, will the Government disclose the exact test methods and tailoring required for JEDI Tactical Edge Category One (iii.1) and Category Two (iii.2) operations?	The Definitions Attachment and SOO explain that ruggedized means that the system is specifically designed to meet or exceed MIL-STD-810G standards to ensure reliable operations in harsh usage conditions. Whether the system needs to be tested and certified as meeting the standard is at the discretion of the Government. The testing methods will likely be Military Service specific.
1509	Draft RFP Section L	Section L7: Volume V	Factor 9 (Demonstrations)	98	3718	The Government indicated Offerors would be notified at least 7 calendar days prior to the demonstrations. Additionally, Offerors invited to provide demonstrations will be given 24-hour notice of specific scenarios to be demonstrated for evaluation purposes. To give Offerors time to manage the logistics of having the right resources available in Washington D.C. for the demonstration, will the Government consider providing a larger pool of scenarios from which the specific scenarios to be demonstrated may be drawn from at the same time the notification is given (i e., at least 7 calendar days prior to the demonstration)?	The requirement remains as stated.
1515	Draft RFP Section L	Section L5: Volume III	Factor 3 (Tactical Edge)	95	3562	Can the Government provide the power requirements and physical dimensions suitable for the range of military operations?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1516	Draft SOO	4 Performance Requirements	4.27	9	356	If the Government's intent is to utilize its already-acquired licenses in the "bring your own license" approach and will be responsible for validating the license, what is the Government's procedure for verifying that the software license is valid and being used in accordance with the End User License Agreement?	The responsibilities for licensing terms and conditions for third party offerings in the marketplace are clarified in the Section H clause entitled "Third Party Marketplace Offerings" in draft RFP #2.
1517	Draft RFP Section I	I	252 227-7028	29	N/A	What is the Government's rationale for including DFARS 252.227-7028 Technical Data or Computer Software Previously Delivered to the Government? This clause is not applicable, was previously issued in 1995 and was not intended to apply to cloud services, also the clause only applies to non-commercial items – see DFARS 227.7103 and SBIR programs.	It is posible that an Offeror may have already delivered some of the materials required by the CDRLs, i e., technical data, under another Government contract.
1518	Draft RFP Section I	I	252 239-7001	29	N/A	What is the Government's rationale for including DFARS 252.239-7001? This clause is not applicable is it applies to specified information assurance functional services, not cloud services – see DFARS 239.7102-3.	This clause has been removed.
1519	Draft RFP Section H	Section H13: Mandatory Addendum License Agreement or Terms of Use	H13	26-27	454-489	H. 13 "Addendum to License Agreement or Terms of Use" states: "and only to the extent those terms meet the Government's needs". Are the "Government's needs" limited to the Government's needs identified in the Performance Work Statement that will be incorporated into the awardee's contract?	The Government's needs are the requirements in the Performance Work Statement incoporated at contract award and the Cyber Security Plan.
1551	Draft RFP Section J	PWS Task Order 001	1 2	1	16	The government stated that the CCPO will take actions to ensure cloud security through log analysis, scans and audits. Has the government considered the use real-time risk adaptive protection of their cloud environment for using advanced data analysis for improving security posture with less resources?	The Department will not comment on the methods it will use to ensure information security, but will consider all tools available to ensure the security of data in the cloud.
1552	Draft RFP Section J	PWS Task Order 001	1 2	1	16, 20	The government stated that the CCPO will take actions to ensure cloud security through log analysis, scans and audits and the use of davanced data analysis. Has the government considered the use of accredited cross-domain log analysis enabling combined log analysis of many security domains within a single pane of glass ?	The Department will not comment on the methods it will use to ensure information security, but will consider all tools available to ensure the security of data in the cloud.
1553	Draft RFP Section J	PWS Task Order 001	1 2	1	20,21	The government stated that the CCPO may need to vet new technologies and experiment with new data analysis tools. Has the government considered the use of accredited cross-domain real-time modeling and simulation tools used within range environments today in order to support advanced vetting, testing and experimentation of said tools?	The Department will consider all tools available to ensure the security of data in the cloud.
1554	General	0	0	0	0	Previous questions have been asked about migration and some other services, which the Government informed industry are not part of the JEDI contract scope. Can the Government also confirm that the services below are to be addressed by Government personnel and other programs/contracts, and are excluded from JEDI's scope? 1) Cloud migration planning services and services designed to produce governance, policy, or regulations. 2) Capturing portfolio inventories and dependencies? 3) Measuring application cost, technology and performance? 4) Analyzing options, developing roadmaps, business cases and detailed action plans? 5) Executing individual transformations as part of a program to migrate?	All migration activities are out of scope for the JEDI contract.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1555	General	0	0	0	0	Within the current draft Cyber Security Plan and Statement of Objectives, it is not clear which organization bears the responsibility for authorization and accreditation of the individual systems migrated to and hosted in the JEDI cloud. Please identify who has that responsibility.	System/Application owners are responsible for receving an ATO for their system/application.
1556	General	0	0	0	0	Will the Government provide a mechanism or process (either automated or manual) for defining the attributes and roles of individual systems (i e. governance) such that the appropriate levels of data separation and security can be maintained throughout the deployment and operations of the hosted systems in the JEDI cloud?	System/Application owners are responsible for assigning the attributes, roles, and permissions for their system/application; however, the Offeror must provide highly granular role-based access control (RBAC) configuration for use by those owners.
1557	Draft RFP Section L	L6	Factor 8	97	3681	The RFP suggests that the contractor is required to maintain a 20% SB requirement for CL NS x00401 and x00501 throughout the life of the contract. These CL Ns are the classified support package and the portability plan. The Q&A from draft RFP 1 stated that this SB requirement would be limited to the Cloud Support Package CLINS which are x00301 and x00401. Please clarify where the SB requirement resides.	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation, which only applies to the Unclassified Cloud Support Package CLINs.
1558	General	0	0	0	0	The Government's comments in the answers to questions repeatedly refers to "AT-AT", for example describing it as "The DoD's provisioning tool, known as the Account Tracking and Automation Tool (AT-AT), will manage user identity, access control, billing configuration, and security and configuration policy compliance for the purposes of accessing the JEDI Cloud." AT-AT is not mentioned in the Draft RFP documents such as the SOO and Solicitation document. Can the Government clarify the scope of AT-AT by documenting detailed specifications and scope in the solicitation to ensure that all Offerors propose their solutions to a common set of requirements?	The Department is responsible for updating and maintaining the AT-AT provisioning tool. Integration with the cloud provider will be achieved through the Offeror provided application programming interfaces (APIs) described in Section L and required in the SOO.
1559	General	0	0	0	0	A single award solicitation of this magnitude will require at least two years to begin to realize ROI within DoD. Unlike what some DoD leadership have suggested, this guarantees the solicitation will extend well into the future. A multi-cloud environment in which the major cloud providers are all required to collaborate would be a much more effective and viable approach to implementing cloud in the DoD. A cloud collaboration between the major vendors would provide a wide range of innovative solutions that would propel the DoD into a third off-set.	Your comment has been noted.
1560	General	0	0	0	0	A multi-cloud approach would prevent a single cloud provider from establishing cultural perceptions, processes and policies that would increase the costs and effort to invite additional cloud providers into the DoD. A multi-cloud approach would require platform vendors to work together to overcome common infrastructure challenges – for example, best approach for CAP access, cybersecurity monitoring, network modernization and cross cloud brokering. We recommend the government use a multi-cloud approach.	Your comment has been noted.
1561	General	0	0	0	0	A single cloud provider award has the potential for DoD overcommitting to one vendor and potentially establishing an industry expectation that would virtually exclude future competition and innovation by freezing out other platform providers. To ensure a fair and open competition, we recommend the government pursue a multi-cloud, multi-award approach.	Your comment has been noted.
1562	General	0	0	0	0	This solicitation has been characterized as a "pathfinder" by DoD leadership. If that were really true, then the IDIQ would focus on building CAP access to the primary vendors within the commercial cloud instead of such a massively broad solicitation and set of requirements that include building an on-premise IL-6 cloud and focusing on edge capabilities. To reduce risk to the taxpayers and the warfighter community, we recommend changing the solicitation to incrementally implement cloud capabilities using an agile approach.	Your comment has been noted.
1563	General	0	0	0	0	This RFP has been gated and specified in a way that is intended to advantage AWS over other cloud providers. The requirements intentionally attempt to exclude vendors who have created innovative solutions that automate DevOps and PaaS to effectively reduce the amount of integration necessary managing big data and for building AI and Analytics solutions in the cloud. This is no more evident than in the marketplace requirements and the requirement to separate PaaS from the underlying IaaS environment. We suggest modifying the marketplace gate to be vendor agnostic.	The RFP is based on DoD's requirements. Your comment has been noted.
1564	General	0	0	0	0	The RFP is overly complex and broad for an experimental "pathfinder"-like environment. Execution of the requirements defined herein will overly tax any of the large cloud providers and is too risky. Cost recovery by cloud platform providers comes in years 6 to 10 after deployment of a cloud data center. The vendor may well never recoup sunk costs to address the requirements in the RFP. This could undermine the future success for cloud deployment within the DoD. The DoD should focus on incremental success with multiple cloud providers instead of one gigantic overly risky single award.	Your comment has been noted.
1565	General	0	0	0	0	How will the contracting agency quantify and mitigate the application migration cost risk presented by a dependency on a single cloud platform?	Transition and migration services are outside the scope of the contract.
1566	General	0	0	0	0	Because the RFP is a publicly available document, the assumption is that non-US citizens may participate in the creation and development of a proposal. Is this assumption correct?	The Offeror will determine who creates or develops their proposals.
1567	General	0	0	0	0	How will the contracting agency adjust effective price in recognition of the widely disparate application migration costs and prices dependent on differing cloud platforms?	Transition and migration services are outside the scope of the contract.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1568	Draft SOO	3	2 Scope	3	113	Section 2 of the Draft SOO calls out 8 objectives for this solicitation. This includes "2 8 Advanced Data Analytics: An environment that securely enables data-driven and timely decision making at the tactical level (within a single data domain) and strategic level (across data domains) and supports advanced data analytics capabilities such as machine learning and artificial intelligence." However, the only other mentions of Data Analytics in the SOO are performance requirements on (4.24, page 9) and (4 32, page 10). There are no mentions in the SOO Scope section. In the Solicitation document, there are no mentions in section C. Section L includes a mention as part of gate factor 1.6 Commercial Cloud Offering Marketplace, and Factor 3 - Tactical Edge. There is no mention of Data Analytics in Section M, Evaluation Criteria. We agree that Data Analytics is critical to the Government's success for the JEDI program. Would the Government consider better defining this objective, including adding language to the Scope section, and expanding the instructions and evaluation criteria to allow Offerors to bid to the same set of requirements and evaluation criteria?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution. The requirement remains the same.
1569	Draft SOO	4	4	6	207	The longest part of the accreditation process is Government and 3rd party approvals. Current timelines suggest that the provider must already have data centers that are already approved or are well into the process of receiving 3rd party and Government sign-off to meet this requirement which essentially limits competition to two providers. If the government wants a fair and open competition, we highly recommend the Government amend the timelines to only include what the offeror can control which is to be compliant with security control requirements of their commercial data centers within a given time frame and not require final FedRAMP compliance as it requires Government and third-party support dependencies that are out of the control of the offerors.	Your comment has been noted.
1570	Draft SOO	4	4	6	207	Line 207 of the SOO states "the proposed solution must be available and meet accreditation and authorization requirements within 30 days of contract award for unclassified services" which appears to contradict Section L4 1 2 which states the provider must have no fewer than three EXISTING FedRAMP moderate data centers. Please clarify if the requirement is for the three FedRAMP Moderate commercial data centers to be accredited at time of submission or within 30 days of award as indicated in the SOO? To ensure a fair and open competition, we recommend the government allow commercial data centers to be available and meet accreditation and authorization requirements within 30 days of contract award for unclassified service to prevent limiting the number of CSPs that can bid to only AWS and Microsoft.	Sub-factor 1.2 has been clarified and updated in the final RFP. Additionally, the applicable FEDRAMP requirements have been clarified in the Cyber Security Plan.
1571	Draft CyberSec Plan	4	4	4	113	To ensure applications and associated data can only be leveraged in approved locations, it is recommended that the government require that virtual machines can only decrypt and run on specific approved servers, in approved locations, with Trusted Platform Module hardware.	Your comment has been noted. The requirement remains as stated.
1572	Draft CyberSec Plan	4	4.2.5	5	151	To what architectural layer does the requirement for "Highly granular access control configuration for compliance with technical policies" refer? Is this a requirement for building applications on the cloud?	The highly granular access control configurations requirements refer to the virtual enclave, application, and data access layers. The Department is looking for Offerors to provide innovative products and services that meet the solicitation requirements while following industry standards and best practices.
1573	Draft CyberSec Plan	4	4 3	5	155	To ensure cloud hosted servers are configured securely, it is recommended that the government require a "root of trust" confirmation on every server reboot, using a hardware Trusted Platform Module (TPM). This ensures that computer firmware, BIOS and container environment have been verified as unchanged, matching a reference for each of these elements.	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1574	Draft CyberSec Plan	4	4 3	5	155	To ensure cloud hosted servers are secure, it is recommended that the government require virtual machines including data, application and operating system combination within, can only run on servers where "root of trust" has been verified.	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1575	Draft CyberSec Plan	4	4.4	5	161	To effectively secure DoD workloads and network communication, the government must have the ability to operate and manage cloud connectivity using a dedicated network, without traversing the public internet. Requirements must be updated to require CSPs to separate operational networks from the public internet.	Your comment has been noted. The requirement remains as stated.
1576	Draft CyberSec Plan	4	4 5	6	179	Please provide an example of a logical component within a supply chain.	Source code access with edit history and attribution.
1577	Draft CyberSec Plan	C	C.3	10	270	In this context is "FedRAMP Moderate or FedRAMP High Compliant" equivalent in meaning to "FedRAMP Moderate or FedRAMP High Authorized"? Or is the DoD intent to allow the vendor to be compliant to the FedRamp requirements in order to obtain a DoD Authority to Operate - in this case already having a FedRamp pATO or ATO would not be required? To ensure a fair and open competition, we recommend the government allow the vendor to be compliant with the FedRAMP requirements and allow the vendors to become authorized within a timeframe that the government can meet.	The word choice between compliant versus authorized is deliberate. The Cyber Security Plan does not require prior accreditation or certification. This has been clarified in the Final RFP.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1578	Draft CyberSec Plan	C	15	10	294	Please expand on what is intended by "Assessments and attacks to verify security compliance and incident response" - This is very vague.	The Department is looking for vendors to provide innovative products and services while following industry standards and best practices.
1579	Draft RFP Section C	C	C.2 Program Management	14	157, 158	Subsection c states "Program Management is an overarching management requirement for the D/IQ and is not separately priced or billable." However, the list of deliverables in SOO section 5.2 contains some items with CL N numbers (e g. Portability Plan), other items that are listed in section C.2 (e.g. Monthly Progress Report), and others that are neither listed in C.2 nor have corresponding CLIN numbers (e g. Capability Update Plan). Can the Government please clarify the PMO role to indicate which deliverables are billable vs not billable so that all vendors price the same set of deliverables?	The Program Management support function has been clarified in the SOO and added as a separate CLIN to the RFP.
1580	Draft RFP Section C	4	d	15	174	The inclusion of Clause C4 sub-section D effectively eliminates the potential for cloud service providers to team with one another in a prime contractor/sub contractor relationship to provide an integrated solutoin for the Government. Because of the nature of this market, No CSP will ever provide another CSP with "unrestricted physical access" to their data centers nor will the CSPs be able to meet the 8 hour requirement. To ensure the government can receive the most capability for the warfighter, we recommend this clause be removed immediately to allow for effective teaming relationships between cloud providers.	Your comment has been noted.
1581	Draft RFP Section H	0	0	0	0	DoD has stated that they will do a re-look at the single award DIQ at the end of the 2 year base; given the comment, will DoD add an on-ramp clause to allow for additional offerors that has been utilized in various DoD large DIQs?	The requirement remains as stated.
1582	Draft RFP Section L	L4	1 2	89	3303	Factor 1.2 in Section L states the provider must be "FedRAMP moderate compliant" at "No fewer than three physical, existing unclassified data center locations" which seems to be in contradiction with SOO Section 4, 4 0 Line 207, which provides a timeline of 30 days post award for the UNCLAS services to "meet accreditation and authorization requirements." Please clarify, are the three FedRAMP moderate data centers required to be accredited upon submission or 30 days post award as this contradiction significantly changes the level of competition for this acquisition. To ensure a fair and open competition, we recommend the government follow the language of the SOO which allows commercial data centers to be available and meet accreditation and authorization requirements within 30 days of contract award for unclassified services, to prevent limiting the number of CSPs that can bid to only AWS and Microsoft.	Sub-factor 1.2 has been clarified to require FedRAMP Moderate Approved by the JAB for purposes of the Gate Criteria. The security requirements for the unclassified environment have been clarified in the Cyber Security Plan, which sets a standard higher than FedRAMP Moderate compliant. The Government will work closely with the awardee to facilitate post-award security accreditation and authorization.
1583	Draft RFP Section L	L4	1 2	89	3303	Factor 1.2 in Section L states: "No fewer than three physical, existing unclassified data center locations within the Customs Territory of the United States." Due to the Government authorization process, this requirement essentially limits competition to two cloud providers. If three data centers are actually required, we suggest changing this requirement to TWO physical existing unclassified data center locations with a third data center available 90 days post award - which would open the competition to more global commercial cloud providers not just AWS and Microsoft.	The requirement remains as stated.
1584	Draft RFP Section L	L4	1 5	91	3367	Clarify expectation regarding "Reading Network Utilization." Do you require the percent utilization (ie % of available bandwidth) or current network throughput (ie bps)?	This requirement has been removed from Section L, subfactor 1 5 in the final RFP.
1585	Draft RFP Section L	L4	1 5	91	3367	Are you looking for a single value (average) for the period specified by the range or a series of averages? If so, what would the period used to average be?	This requirement has been removed from Section L, subfactor 1 5 in the final RFP.
1586	Draft RFP Section L	L4	1 5	91	3368	Please describe in more detail the potential length of expected time and date range? (hours, days, weeks, months, years)	This requirement has been removed from Section L, subfactor 1 5 in the final RFP.
1587	Draft RFP Section C	4	0	15	174-202	Publically available Commercial Cloud Computing infrastructure is tightly controlled and proprietary to the Owner. Granting outside control and access for the purpose of security will result in an opposite outcome that is less secure and controlled. The reference to unclassified environment should be removed from C4.c. Section C4.d.ii should be applicable for the classified environment only. For the unclassified environment, it is recommended that the Prime contractor have a bilateral signed agreement with the Owner to convey and to measure the timeliness for implementing critical security vulnerabilities.	The Section C4 control requirements remain as stated.
1588	Draft RFP Section L	6	Factor 8	98	3688	The small business requirement is stated to be based on 20% of TCV of awards for CL N 401 and CL N 501. This looks incorrect and should reference CLIN 301 and CLIN 401 for Cloud Support Packages.	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation, which only applies to the Unclassified Cloud Support Package CLINs.
1589	Draft CyberSec Plan	General	0	0	0	Contractor recommends dividing the Cyber Security Plan into unclassified and classified that maps to the government's CL N Structure. The Government will benefit from a clearer and more concise security plan for each security level and more enforceable and tangible requirement for accountability. There additional controls on classified side that don't have relevance to the unclassified side. The single Cyber Security Plan places undo burden and cost on the government to enforce.	The Government has declined to separate out the requirements as recommended, but has attempted to clarify any ambiguities.
1590	Draft CyberSec Plan	4	4.1	4	125	As written, this states that physical access to infrastructure is equivalent to logical root access of systems. Did the government intend this statement to reference that physical access to infrastructure is equivalent to physical root access and not logical system access?	The Cyber Security Plan has been updated. The statement about physical access equating to logical access has been removed.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1591	Draft CyberSec Plan	4	4.1.4	5	135	t is highly recommended the government split unclassified and classified requirements into two sections. The requirements for a classified non-network infrastructure are not the same as the requirements for an unclassified infrastructure. We recommend breaking requirements down by unclassified and classified that maps to the government's CL N Structure. The government will get a concise security plan for each security level, which will be more enforceable. There should be more controls on the classified side that don't need to be implemented on the unclassified side. More so, this requirement is in conflict with the requirements of FedRAMP High.	The Government has declined to separate out the requirements as recommended, but has attempted to clarify any ambiguities.
1592	Draft CyberSec Plan	4	4.1.5	5	137	"No individual may have both physical and logical access." Can the government please confirm their definition of logical access means customer workloads.	The approved Cyber Security Plan has been updated to clarify the Government's requirements.
1593	Draft CyberSec Plan	4	4.5.0	6	179	"4.5.0 The CIO may require specific physical and logical component supply chains." DoD intends to leverage commercial cloud infrastructure for unclassified workloads. The CSPs cannot accept specific supply-chain change requests as it will dramatically impact the public cloud offering which is purpose built. This requirement is more applicable to the classified infrastructure and the tactical edge and should be stated as such. More so, can the government please clarify how this requirement is intended to apply to a Saas/IaaS offer, as supply chain reviews are normally associated with the delivery of commodities.	This is a critical security requirement. The Government is not intending to unnecessarily interfere with the cloud vendor's public offerings; however, there are instances driven by security concerns, such as the recent issue around Kaspersky software, that may result in specific supply chain requirements, which will also benefit the vendor's other commercial clients given the underlying security issue.
1594	Draft CyberSec Plan	4	4.5.1	6	181	"The CIO may require specific traffic profiles be intercepted, modified, or stored." To avoid putting other cloud customers at risk, this sentence should have a bound scope by stating that it is limited to JEDI applications and infrastructure traffic only.	The approved Cyber Security Plan has been updated to clarify the Government's requirements.
1595	Draft CyberSec Plan	4	4.5.9	6	197	To improve clarity of this section we recommend the following, "The CIO determines priority between mitigations, then investigations, then testing of customer workloads."	This requirement has been clarified in the final RFP.
1596	Draft CyberSec Plan	C	C.4	10	272	"Classified infrastructure - FedRAMP High compliant for all classification levels." FedRAMP High is achievable and does not require US Data Location requirements. It would appear that the government is using FedRAMP High and IL interchangeably when they are not.	The security requirements pull from multiple sources to reflect the totality of JEDI Cloud's requirements as described in the Cyber Security Plan, which has been clarified for the final RFP.
1597	Draft CyberSec Plan	C	C.4	10	272	The statement for Classified infrastructure should state FedRAMP High for all classified levels. t incorrectly states "all classification levels."	This requirement has been clarified in the final RFP.
1598	Draft SOO	3	3.12	4	164	Log data is proprietary information to the CSPs. Cloud service providers will not authorize a blanket request of all log data to any customer, so we need to understand what types of access the government will be requesting. Can the government please provide guidance around what types of log data will be requested?	Information security is critical to the operations of the Department of Defense. The final RFP clarifies the Department's requirements regarding hypervisor access and logs in the Cyber Security Plan and SOO.
1599	General	0	0	0	0	The government should understand that the marking of an issue as "critical" should be understood as a technical or contractual roadblock for the vendor to participate as a prime or subcontractor for the JEDI acquisition. Without government consideration and flexibility, it will result in a no-bid position reducing the participation and competition for this award.	The vendor's clarification is noted.
1600	Draft SOO	2. Scope	2.7	3	110	Language for "by default" was removed from Section L, Sub-factor 1.4 Logical Isolation, per DRFP1 Q&A 775. We request that it be removed from here, as well. Leading CSPs provide cryptographic capabilities for traffic and data at the application level. It is our experience that the majority of customers who want cryptographic capabilities prefer to implement and maintain control of their own inter-process key management and data transfer encryption. They prefer this approach because it allows them a greater level of control over their data (i.e., customers choose what algorithms they want to use and in which mode they use those algorithms and choose how they generate and protect their encryption keys).	The SOO has been updated to clarify the Department's requirement.
1601	Draft SOO	3. Performance Objectives	3.10	4	157-158	While CSPs provide customers with the ability to create reports, we understand from the DRFP that the intent of the Government's AT-AT tool is to perform this function. Can the Government please clarify that this assumption is correct?	The AT-AT provisioning tool will be a conduit for providing various reporting information to Department customers. The Offeror must ensure the requirements stated in the SOO are met in order to enable this reporting.
1602	Draft SOO	4. Performance Requirements	4 6	6	232-234	While CSPs provide customers with the ability to perform this function, we understand from the DRFP that the intent of the Government's AT-AT tool is to perform this function. Can the Government please clarify that this assumption is correct?	The AT-AT provisioning tool will be a conduit for providing various reporting information to Department customers. The Offeror must ensure the requirements stated in the SOO are met in order to enable this reporting.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1603	Draft SOO	4. Performance Requirements	4 9	7	255-261	This section requires the Contractor to report JEDI "usage" relative to the Contractor's "total usage" in its Monthly Report to the Cloud Computing Program Office in order to demonstrate that DoD usage constitutes less than 50% of the Contractor's total usage. CSP usage statistics could implicate material, non-public information. We suggest that the Contractor be permitted to certify to the fact that DoD usage constitutes less than 50% of the Contractor's total usage. Alternatively, DoD could permit the Contractor to certify compliance with this requirement so long as DoD usage does not approach the 50% threshold (e.g., DoD usage is less than 25%) and only provide detailed usage statistics if DoD usage approaches 50%. This approach would prevent Government personnel from unnecessarily having access to potential insider trading information and would protect the Contractor's confidential, sensitive business information.	The requirement to maintain a certain level of utilization will be removed for the final RFP, but regular reporting about utilization levels will remain. Any proprietary information contained in contract deliverables should be marked as such in accordance with the contract's data rights clauses.
1604	Draft SOO	4. Performance Requirements	4.22	8	310	Please confirm that the Government intended CLIN x00106.	The CLIN numbering has been updated in the final RFP.
1605	Draft SOO	4. Performance Requirements	4.22	8	311	Please confirm that the Government intended CLIN x00105.	The CLIN numbering has been updated in the final RFP.
1606	Draft SOO	4. Performance Requirements	4.26	9	352	We request that the Government revise Line 352 to state "Provisioning an offering from this marketplace " CSPs facilitate marketplaces that include third-party software and services where provisioning times are dependent upon configurations that the CSP does not control. For example, if a third-party product uses templates that provision the CSPs' services on top of the core virtual machine (VM), this will extend the time it takes to fully provision the offering.	This requirement has been clarified in the final RFP.
1607	Draft SOO	4. Performance Requirements	4.34.1	10	396-399	Leading CSPs provide customers with encryption capabilities and allow customers to determine what data requires encryption consistent with their security posture and requirements. This approach allows customers to implement and maintain control of their own inter-process key management and data transfer encryption. It also allows for a greater level of control over their data (i.e., customers choose what algorithms they want to use and in which mode they use those algorithms and choose how they generate and protect their encryption keys). To ensure that DoD retains that flexibility and control, we recommend the following wording: "The Offeror must provide the ability to encrypt data at rest and data in transit, such that users can choose to require the implementation of up to two layers of commercial grade encryption using algorithms and procedures specified in Committee on National Security Systems Policy (CNSSP) 15."	The final SOO and Cyber Security Plan has been updated to clarify the Government's requirements.
1608	Draft SOO	5. Performance Metrics	Table 5.1, tem 6	13	Entirety	CSPs do not launch updates across their entire global footprint in a short time, even in their commercial regions. Doing so would be unwise because it could increase the impact radius of potential flaws that may need to be rolled back after partial deployments. We recommend the following wording: "Action plan to patch application and updates to underlying infrastructure and cloud services for critical updates (subject to negotiation)."	A definition of commercial parity has been added to the Definitions Attachment, which scopes the definition to the continental United States.
1609	Draft SOO	5. Performance Metrics	Table 5.1, tem 9	14	Entirety	tem 9 attempts to define a single objective for billing and usage metrics and then establishes a standard for usage and reporting. This standard is feasible for usage and reporting, but not for billing. We recommend removing references to billing from the item's Objective and Monitoring Method columns.	The metrics for billing and usage have been separated.
1610	Draft SOO	5. Performance Metrics	Table 5.1, tem 10	14	Entirety	tem 10 can imply that the Government intends to value the availability of the API (i.e., the ability to modify the state of running services) over the availability of the service. We suggest that this metric be reworded to describe overall service availability. Today, commercial CSPs do not offer 99 999% service availability (i.e., systems offline for no more than six minutes a year) service level agreements.	The 99.999% in item 10 of table 5.1 refers only to the uptime of the API systems supporting the cloud offering. tem 10 does not refer to the uptime of the underlying cloud service infrastructure.
1611	Draft SOO	5. Performance Metrics	Table 5.1, tem 12	14	Entirety	The experience of CSPs has shown that while this is a laudable goal, it is not actually achievable. This metric should be expressed as an "important, best efforts" goal but not as an absolute requirement. For example, Government compliance requirements often make this metric impossible to meet. In addition, and more broadly, CSPs do not launch updates across their entire global footprint in a short time, even in their commercial regions. Doing so would be unwise because it could increase the impact radius potential flaws that may need to be rolled back after partial deployments.	The performance metrics about commercial parity have been clarified to measure based on ready for IV&V testing. Definitions for IV&V testing and commercial parity have been added to the Definitions Attachment.
1612	Draft SOO	5. Performance Metrics	Table 5.1, tem 13	14	Entirety	The experience of CSPs has shown that while this is a laudable goal, it is not actually achievable. This metric should be expressed as an "important, best efforts" goal but not as an absolute requirement. For example, Government compliance requirements often make this metric impossible to meet. In addition, and more broadly, CSPs do not launch updates across their entire global footprint in a short time, even in their commercial regions. Doing so would be unwise because it could increase the impact radius potential flaws that may need to be rolled back after partial deployments.	The performance metrics about commercial parity have been clarified to measure based on ready for IV&V testing. Definitions for IV&V testing and commercial parity have been added to the Definitions Attachment.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1613	Draft SOO	5. Performance Metrics	Table 5.1, tem 16	15	Entirety	We request that the Government modify this requirement to state, "Make best efforts to offer latest DBMS software " CSPs have no control over when a vendor will update their marketplace offerings.	The Government is referring to DBMS offerings provided as part of the Offeror's IaaS and PaaS offerings rather than those provided in the online marketplace. The language in the SOO has been updated to reflect this clarification.
1614	Draft SOO	5. Performance Metrics	Table 5.1, tem 19	15	Entirety	Please confirm that the Government intended CLIN x00105.	The CLIN numbering has been updated in the final RFP.
1615	Draft SOO	5. Performance Metrics	Table 5.1, tem 21	15	Entirety	We request that the Government change the Objective to "Marketplace offering time to provision." CSPs facilitate marketplaces that include third-party software and services where provisioning times are dependent upon configurations that the CSP does not control. For example, if a third-party product uses templates that provision the CSPs' services on top of the core virtual machine (VM), this will extend the time it takes to fully provision the offering.	This requirement has been clarified in the final RFP.
1616	Draft SOO	5. Performance Metrics	Table 5.1, tem 24	15	Entirety	We request that the Government modify this requirement to state, "Make best efforts to make publicly available marketplace offerings available " Determining which marketplace offerings are available in a particular unclassified environment is a shared responsibility between the marketplace vendor and the CSP and is subject to factors outside of the CSP's control. For example, a marketplace vendor may choose not to make their unclassified offering available in every unclassified environment around the globe due to business or legal reasons.	The scope of third party marketplace offerings has been updated in the SOO. Also, the relevant performance metrics have been clarified to measure based on ready for IV&V testing.
1617	Draft SOO	5. Performance Metrics	Table 5.1, tem 25	16	Entirety	We request that the Government modify the Standard to state, "Upon Government approval." Determining which marketplace offerings are available in classified regions is a shared responsibility between the Government, the marketplace vendor, and the CSP and is subject to factors outside of the CSP's control. For example, a marketplace vendor may choose not to make their unclassified offering available in a classified environment, or the Government may not approve the inclusion of an offering in the classified marketplace. Additionally, a vendor must take several steps to make an unclassified offering compliant with a classified environment, which generally takes longer than 30 days.	The online marketplace requirements have been clarified in the SOO. The performance metric has also been updated.
1618	Draft SOO	5. Performance Metrics	Table 5.1, tem 28	16	Entirety	Can the Government clarify the data storage type this would apply to?	RPO / RTO apply to all data storage types.
1620	Draft CyberSec Plan	1. Compliance	1.1.4	3	85	Does DoD intend for unclassified commercial CSP infrastructure used by private commercial entities to be part of the DoD N? We believe that DoD workloads and their virtualized environments are considered part of the DoDIN, but not the CSP's physical infrastructure on which those workloads run.	The Cyber Security Plan with the final RFP establishes that JEDI infrastructure is considered part of the greater DoD N. The requirements regarding infastructure access and other security related considerations have been clarified in the Cyber Security Plan and contract clauses.
1621	Draft CyberSec Plan	3. Modernization	3.0	4	108	This section is unnecessary because DoD will be buying commercial capabilities. Leading CSPs make new cloud service offerings available in different regions based on customer demand. This allows CSPs to properly allocate resources and ensure that services are implemented at a sufficient scale, capacity, and volume to meet customer demand. Ceding control of this process to the Government—particularly with regard to unclassified regions—is inconsistent with the commercial nature of the services required by the DRFP. We recommend removing this section.	A definition of commercial parity has been added to the Definitions Attachment. The modernization requirements have been clarified.
1622	Draft CyberSec Plan	4. Requirements	4.1.5	5	137	We suggest that DoD change this requirement as follows: "No individual may have both physical access to infrastructure and logical access to customer data. In the event of an emergency that requires an individual to access both, the CSP will follow emergency access protocols and obtain appropriate management authorization before taking necessary steps required by the emergency and will follow security incident reporting procedures as specified in the Cyber Security Plan for any incident involving Government data."	The approved Cyber Security Plan has been updated to clarify the Government's requirements.
1623	Draft CyberSec Plan	4. Requirements	4.2.1	5	143	Leading CSPs provide customers with encryption capabilities and allow customers to determine what data requires encryption consistent with their security posture and requirements. This approach allows customers to implement and maintain control of their own inter-process key management and data transfer encryption. It also allows for a greater level of control over their data (i.e., customers choose what algorithms they want to use and in which mode they use those algorithms and choose how they generate and protect their encryption keys). To ensure that DoD retains that flexibility and control, we recommend the following wording: "Ability to encrypt data at rest and in transit pursuant to Committee on National Security Systems Policy (CNSSP) 15 [D 3]."	The final SOO and Cyber Security Plan has been updated to clarify the Government's requirements.
1624	Draft CyberSec Plan	4. Requirements	4.2.4	5	149	We recommend updating this language as follows: "Authentication to classified infrastructure requires DoD PKI, Multi-Factor Authentication (MFA), or other mutually agreed upon alternative authentication technology." This will allow DoD to maximize competition and take advantage of the most advanced authentication technologies without needing contract modifications or sacrificing security.	DoD PKI remains required for classified authentication.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1625	Draft CyberSec Plan	4. Requirements	4.5.0	6	179	CSPs manage supply chain hygiene as an integral aspect of ongoing compliance with applicable security rules and regulations (e.g., DoD SRG, FedRAMP). Furthermore, physical and logical component sourcing may impact a CSP's ability to deliver commercial cloud services and may have a significant impact on pricing. We suggest this requirement be revised as follows: "The CIO may request specific physical and logical component supply chains. The Contractor shall make all reasonable efforts to comply with the CIO's requests." This language strikes a balance between DoD's security requirements and the commercial nature of the services.	This is a critical security requirement. The Government is not intending to unnecessarily interfere with the cloud vendor's public offerings; however, there are instances driven by security concerns, such as the recent issue around Kaspersky software, that may result in specific supply chain requirements, which will also benefit the vendor's other commercial clients given the underlying security issue.
1635	Draft RFP Section J	Definitions	9	1	23-24	Classified infrastructure is defined as "FedRAMP High compliant infrastructure;" however, the FedRAMP High baseline does not apply to classified infrastructure. According to FedRAMP, FedRAMP High applies to "the Government's most sensitive, unclassified data." We recommend updating this definition to make it consistent with FedRAMP. This will reduce significant ambiguities throughout the documents and will allow DoD to take advantage of CSP infrastructure that already possesses a FedRAMP High authorization.	The approved Cyber Security Plan has been updated to clarify the Government's requirements.
1636	Draft RFP Section J	Draft CDRLs	Box 2	1	Entirety	Can the Government confirm that the Monthly Status Report (MSR) is the same as the Monthly Progress Report (defined in DRFP Section J, Page 56) mentioned in the SOO Table 5 2, tem 1?	These are the same documents. The terminology has been updated for consistency.
1637	Draft RFP Section J	Draft CDRLs	Block 12	19	Entirety	Can the Government please confirm that the Contract Ordering Guide is required within 15 days of contract award as stated in the SOO, Table 5.2, Item 10, and not on day one of contract award as stated within Box 12?	It should be 5 days after award. This has been corrected in final RFP.
1638	Draft RFP Section J	Draft CDRLs	tem 12	21	Entirety	Can the Government please confirm that the Implementation Plan is due within 15 days of contract award as defined within the SOO, Table 5.2, Item 11, and not the day after contract award as stated in Box 12?	It should be 5 days after award. This has been corrected in final RFP.
1639	Draft RFP Section J	Draft CDRLs	Block 12	21	Entirety	Can the Government clarify whether the QASP is required on an annual basis as defined here, or on a monthly basis as defined in the SOO, Table 5.2, Item 12?	The QASP is required 30 days after contract award, then annually thereafter.
1640	Draft RFP Section J	Draft CDRLs	tem 12	23	Entirety	Can the Government please confirm that the QASP is due 30 days after contract award as stated in Box 12, and not at contract award as stated in Box 16?	The QASP is required 30 days after contract award, then annually thereafter.
1641	Draft RFP Section J	Draft CDRLs	Block 12	24-26	Entirety	Can the Government please confirm that the Security Authorization Package is due 30 days after contract as defined here, and not at contract award as defined in Block 16?	The Security Authorization Package for unclassified services is due 30 days after contract award. The CDRL has been updated for clarity.
1642	Draft RFP Section J	Draft CDRLs	tem 12	25	Entirety	Can the Government clarify the meaning of DAR? If this is Date After Receipt, can the Government clarify what receipt they are referring to?	The Technical Report is ad hoc and due within 30 days after request by the Government.
1643	Draft RFP Section B	B1: Schedule of Services	CLIN 000105	4	Entirety	Developing a Firm Fixed Price for a Portability Plan will require the scope of what is being ported. We recommend that the Government identify a specific Pricing Scenario that includes export (e.g., Scenario 1(c)) upon which to develop the Firm Fixed Price for this CL N.	Section L under Factor 9 Price has been updated to state that the scope and complexity of the applications and data described in the Price Scenarios are illustrative examples that should inform the pricing of the Portability Test and Portability Plan CL Ns.
1644	Draft RFP Section B	B1: Schedule of Services	CLIN 000105	4	Entirety	The DRFP includes Cloud Support Services, but specifically excludes migration services from its scope. Please confirm that execution of the Portability Plan required in CLIN 000105 would be carried out under a separate migration contract. Likewise, please confirm that any Transition Plan delivered pursuant to Section C3 would be executed under a separate migration contract.	The scope of the Portability Plan does not include actually executing the export. The Portability Plan is intended to be instructional to JEDI Cloud users. Migration services are outside the scope of JEDI Cloud. For clarity, however, the Government would note that the Contractor will be executing the Portability Plan as part of the periodic demonstration required under the Portability Test CL N x006. Additionally, Section C3 has been updated to clarify the Transition Plan requirements and what elements of that Plan would be executed under the JEDI Cloud contract.
1645	Draft RFP Section B	B1: Schedule of Services	CLIN 000106	5	Entirety	Developing a Firm Fixed Price for a Portability Test effort will require the scope of what is being ported. We recommend that the Government identify a specific CSP Pricing Scenario that includes export (e.g., Scenario 1(c)) upon which to develop the Firm Fixed Price for this CL N.	Section L under Factor 9 Price has been updated to state that the scope and complexity of the applications and data described in the Price Scenarios are illustrative examples that should inform the pricing of the Portability Test and Portability Plan CL Ns.
1646	Draft RFP Section B	B2: Maximum Contract Ceiling and Minimum Contract Guarantee		11	95	We believe it is unnecessary for DoD to require the Contractor to maintain a contract price catalog separate from the Contractor's commercial catalog pricing available online. By leveraging commercial price catalogs, DoD can eliminate the need to amend the contract every time the Contractor adds a service or reduces a service price in any of its various regions around the world. Instead, the Government will immediately benefit from new services and reduced pricing when it occurs. Consistent with commercial CSP practices, DoD may negotiate a contractual discount off of the Contractor's commercial catalog pricing.	DoD is bound by acquisition rules that prevent the methodology being proposed.
1647	Draft RFP Section B	B4: Travel		12	Entirety	Work under the Cloud Support Package CLINs is likely to require travel. In order to avoid delays in contract administration and performance, we suggest that the IDIQ base contract permit ordering activities to authorize travel at the order level on a Fixed Price basis. Alternatively, if the Government intends for Offerors to include travel expense in their proposed Fixed Price for Cloud Support Package CL Ns, we suggest that the Government provide an estimate of required travel.	Travel is not intended under the contract.
1648	Draft RFP Section H	H5: New Services		18	323	Please confirm that the term "online catalog(s)" refers to the commercial service catalog that commercial CSPs make available to all users.	This is not intended to refer to the online commerical service catalog available to all users. This language has been clarified in the RFP.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1649	Draft RFP Section H	H6: Price Changes		19	341	Please confirm that the term "online catalog(s)" refers to the commercial service catalog that commercial CSPs make available to all users.	This is not intended to refer to the online commerical service catalog available to all users. This language has been clarified in the RFP.
1650	Draft RFP Section H	H5: New Services		18	Entirety	We believe that this clause is inconsistent with a commercial item acquisition. When a CSP makes a new service available in a classified or unclassified region, that service will immediately be available to DoD at the same commercial item price offered to all customers in that region. We suggest that Clause H5 be replaced with the following: "The Contractor shall make new services introduced in a classified or unclassified region available to DoD at the same commercial item price that the Contractor offers that service to other customers in that region. Any contractual discounts agreed to between DoD and the Contractor shall be applied to new services consistent with the terms of the agreed discount." Alternatively, if DoD does not replace Section H5 in its entirety, we recommend the addition of the following Section H5(d)(ii) regarding pricing for new services in classified regions: "The allowable price for new classified services may be established using the same methodology that the Contractor uses to price the same services in its unclassified regions and include a profit margin that does not exceed the profit margin that the Contractor applies to the same services in its unclassified regions."	The New Services clause in Section H has been revised to simplify the clause. Additionally, the clause is limited to new services made available in the continental United States, which is consistent with the new definition of commercial parity in Attachment J-8 Definitions. The clause also makes the JEDI Cloud Contracting Officer's approval more explicit and invokes the requirements for commercial parity in the Performance Work Statement that will be incorporated at contract award.
1651	Draft RFP Section H	H6: Price Changes		18	Entirety	We believe that this clause is inconsistent with a commercial item acquisition. When a commercial CSP reduces the price of a service in a classified or unclassified region, DoD will immediately get the benefit of that reduced price for all future use of that service in that region. Under commercial CSP business practices, however, a price reduction in one region does not necessarily result in a price reduction for that same service in other regions because variable costs (e.g., power, water, real estate) and utilization profiles vary by region. We suggest that Clause H6 be replaced with the following: "When the Contractor reduces its commercial item price for a particular service in a classified or unclassified region, that reduced price shall be applied to all subsequent DoD usage of that service in that region."	The Price Changes clause in Section H has been revised to simplify the clause. Additionally, the clause is limited to lowered prices made available in the continental United States, which is consistent with the new definition of commercial parity in Attachment J-8 Definitions. The clause also makes the JEDI Cloud Contracting Officer's approval more explicit.
1652	Draft RFP Section H	H13: Mandatory Addendum License Agreement or Terms of Use		21	466-467	In response to comments to the first DRFP, DoD declined to permit Contractors to incorporate service level agreements by reference. We request DoD reconsider its position. t is critical to the commercial business model of CSPs that they retain the ability to make modifications to certain service terms in a manner consistent with their commercial customers. Such modifications are required based on changes to the services or features of services. Additionally, this requirement contradicts the table in Section H13, which has a row on page 24 for "Incorporating other License Terms by Reference, Including Reference to a Website." To strike a balance between DoD's needs and customary commercial practice, permissible changes to incorporated service level agreements could be limited to terms that do not (1) materially affect the Government's obligations, (2) increase Government prices, (3) decrease the overall level of service, or (4) otherwise limit any Government rights addressed elsewhere in the contract. This will ensure that the Government has access to a CSP's latest and most innovative services and features and on terms that are in parity with the Contractor's commercial offerings.	The Section H clause for Mandatory Addendum License Agreement or Service Level Agreement has been updated to incorporate a limited exception allowing certain agreement revisions to take effect prior to incorporation into the contract.
1653	Draft RFP Section H	H14: Third Party Marketplace Offerings	b.	27	Entirety	The definitions of internal and external third-party marketplace offerings are inconsistent with customary commercial CSP business practice. We recommend making the following changes to the definitions: (1) "internal service offerings" should be defined as any offering where the Contractor is the seller of record and (2) "external service offerings" should be defined as any offering sold by a third party. Additionally, with the exception of BYOL offerings, standard commercial CSP business practice is for external service offerings purchased through a CSP marketplace to be billed through the CSP. Billing internal and external marketplace offerings through the JEDI contract will provide the Government with the most flexibility under the contract and reflects how CSP third-party marketplaces function. If the Government would like to separately track marketplace-related costs, a CL N should be added to the contract for marketplace offerings.	The final SOO narrows the scope of required third party marketplace offerings. The Online Marketplace clause in Section H has been significantly updated to clarify the requirement.
1654	Draft RFP Section I	Section I – Contract Clauses	52.204-2	27	Entirety	Please confirm that the requirements of this clause only apply to classified regions. If this clause were to apply to unclassified regions, Offerors would not be able to propose any region without such controls. This would effectively limit DoD to classified regions—even if a Task Order was unrelated to classified information and the Offeror controlled other regions with FedRAMP and/or DoD SRG authorizations sufficient to protect the data.	This clause only applies to classified requirements.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1655	Draft RFP Section I	Section I – Contract Clauses	252 227-7013, 252 227-7015, 252 227-7016, 252 227-7017, 252 227-7028, 252 227-7030	28-29	Entirety	We recommend removal of these clauses, which are contrary to DoD policy and the DFARS. In accordance with DFARS 227.7102-1, DoD is prohibited from acquiring technical data related to commercial services when such data is not customarily provided to the public. Because technical data is not customarily delivered when providing commercial cloud services, these clauses are not applicable. To the extent the Government may believe it needs access to technical data relating to compliance with the PWS, Cyber Security Plan, DoD SRG, and FedRAMP, any permissible access to such data is governed by those documents and standards. If DoD intends to keep these clauses, in accordance with the respective prescriptions, these clauses are only applicable when a contract requires the delivery of specifically identified types of technical data. The DRFP does not identify technical data that falls into the category of technical data identified by the clauses that the Contractor will be required to deliver. What technical data in the categories identified in these clauses will the Contractor be required to deliver under the contract?	The technical data addressed by these clauses are the CDRLs identified in the SOO. Instructions clarifying this intent and explaining how to complete DFARS 252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JAN 2011) have been added to Section L.
1656	Draft RFP Section I	Section I – Contract Clauses	252 227-7014, 252 227-7016, 252 227-7017, 252 227-7019, 252 227-7028, 252 227-7037	28-29	Entirety	We recommend removal of these clauses, which are contrary to DoD policy and the DFARS. In accordance with DFARS 227.7202-1, DoD is prohibited from acquiring technical information related to computer software or computer software documentation not customarily provided to the public. Because such technical information is not customarily delivered when providing commercial cloud services, these clauses are not applicable. To the extent the Government may believe it needs access to computer software or computer software documentation relating to compliance with the PWS, Cyber Security Plan, DoD SRG, and FedRAMP, any permissible access to such data is governed by those documents and standards. If DoD intends to keep these clauses, in accordance with the respective prescriptions, these clauses are only applicable when the Government requires the delivery of specifically identified types of non-commercial computer software or non-commercial computer software documentation. The DRFP does not identify any non-commercial computer software or non-commercial computer software documentation that the Contractor will be required to deliver. What non-commercial computer software and/or non-commercial computer software documentation will the Contractor be required to deliver under the contract?	The technical data addressed by these clauses are the CDRLs identified in the SOO. Instructions clarifying this intent and explaining how to complete DFARS 252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JAN 2011) have been added to Section L.
1657	Draft RFP Section I	Section I – Contract Clauses	252 237-7023, 252 237-7024	29	Entirety	The DRFP does not identify essential Contractor services. t is not possible to provide a Mission Essential Contractor Services Plan without such information. Please clarify if and when DoD will identify essential Contractor services and when any required Mission Essential Contractor Service Plan should be delivered.	These clauses have been removed.
1658	Draft RFP Section I	Section I – Contract Clauses	252 239-7001	29	Entirety	Does DoD have an IA training program that is complaint with this clause that it intends, expects, or will allow the Awardee to use, or is the Awardee expected to independently develop IA training that complies with the requirements of the clause?	This is a contractor responsibility.
1659	Draft RFP Section I	Section I – Contract Clauses	52.203-15	36	Entirety	This clause's prescription states that the clause is only applicable if a contract is funded in whole or in part with Recovery Act funds. We recommend removal of this clause.	This clause has been removed.
1660	Draft RFP Section I	Section I – Contract Clauses	252 237-9000	56	Entirety	We recommend the removal of this clause. Under 10 U.S.C. § 2330a(c), the collection of Contractor manpower data is only required when DoD awards a "staff augmentation contract." The statute defines staff augmentation as "personnel who are physically present in a Government work space on a full-time or permanent part-time basis, for the purpose of advising on, providing support to, or assisting a Government agency in the performance of the agency's missions[.]" See 10 U.S.C. § 2330a(h)(6). None of the services contained within the DRFP fall under the definition of "staff augmentation." Therefore, inclusion of this clause is contrary to FAR 12 301(a) because it is inconsistent with commercial practice and not required by law. Additionally, the inclusion of this clause is impracticable for a cloud infrastructure contract because the services contained within this Firm Fixed Price DRFP are not delivered in a manner that allows for the tracking of labor hours or the maintenance of time-keeping records (see Section 2.5 of Task Orders 1 and 2).	This clause has been removed.
1661	Draft PWS Template	Task Order 1	2 5	2	68-69	We recommend the removal of this clause. Under 10 U.S.C. § 2330a(c), the collection of Contractor manpower data is only required when DoD awards a "staff augmentation contract." The statute defines staff augmentation as "personnel who are physically present in a Government work space on a full-time or permanent part-time basis, for the purpose of advising on, providing support to, or assisting a Government agency in the performance of the agency's missions[.]" See 10 U.S.C. § 2330a(h)(6). None of the services contained within the DRFP fall under the definition of "staff augmentation." Therefore, inclusion of this clause is contrary to FAR 12 301(a) because it is inconsistent with commercial practice and not required by law. Additionally, the inclusion of this clause is impracticable for a cloud infrastructure contract because the services contained within this Firm Fixed Price DRFP are not delivered in a manner that allows for the tracking of labor hours or the maintenance of time-keeping records (see Section 2.5 of Task Orders 1 and 2).	This clause has been removed.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1662	Draft PWS Template	Task Order 2	2 5	2	71-72	We recommend the removal of this clause. Under 10 U.S.C. § 2330a(c), the collection of Contractor manpower data is only required when DoD awards a "staff augmentation contract." The statute defines staff augmentation as "personnel who are physically present in a Government work space on a full-time or permanent part-time basis, for the purpose of advising on, providing support to, or assisting a Government agency in the performance of the agency's missions[.]" See 10 U.S.C. § 2330a(h)(6). None of the services contained within the DRFP fall under the definition of "staff augmentation." Therefore, inclusion of this clause is contrary to FAR 12 301(a) because it is inconsistent with commercial practice and not required by law. Additionally, the inclusion of this clause is impracticable for a cloud infrastructure contract because the services contained within this Firm Fixed Price DRFP are not delivered in a manner that allows for the tracking of labor hours or the maintenance of time-keeping records (see Section 2.5 of Task Orders 1 and 2).	This clause has been removed.
1663	Draft RFP Section I	Section K – Representations, Certifications and Other Statements of Offerors	252 225-7042	80	Entirety	This representation requires Offerors to represent that they are authorized to operate and do business in the country (or countries) in which the contract is to be performed. The DRFP does not identify countries where performance will be required. Please identify the countries in which the Contractor must be authorized to do business prior to award.	This clause has been removed.
1664	Draft RFP Section L	L2: Written Proposal Organization Instructions	5, Table Section III	85	Entirety	Are Offerors allowed 15 pages for each Task Order response (i.e., up to 30 pages total), or 15 total pages for both Task Order responses?	The page limitations have been clarified in Section L. Additionally, the number of task orders has been reduced.
1665	Draft RFP Section L	L2: Written Proposal Organization Instructions	10	87	Entirety	In Section L2 Instruction Number 10, the DRFP states "Information required for proposal evaluation which is not found in its designated volume will be assumed to have been omitted from the proposal. Cross-referencing within a proposal volume across factors or sub-factors is not permitted." The QASP (evaluated under Factor 6 Tab H) and the corresponding PWS in Tab A are interrelated but evaluated as different factors. Please confirm that cross-referencing of the QASP and PWS is permitted.	The Section L instructions have been revised to allow for cross-referencing between the QASP and PWS.
1666	Draft RFP Section L	L3: Volume 1 – Contract Documentation Instruction	General, Tab B	87	3209-3210	Commercial CSPs maintain the exact locations of cloud regions confidential as an integral aspect of physical security. Please confirm that this requirement does not require exact address information for data centers.	Section L has been updated to require an address or GPS coordinates. The proposal will be properly safeguarded from unauthorized disclosure in accordance with the FAR and multiple criminal statues.
1667	Draft CyberSec Plan	4. Requirements	4.6.2	6	Entirety	Commercial CSPs maintain the exact locations of cloud regions confidential as an integral aspect of physical security. Please confirm that this requirement does not require exact address information for data centers.	Section L has been updated to require an address or GPS coordinates. The proposal will be properly safeguarded from unauthorized disclosure in accordance with the FAR and multiple criminal statues.
1668	Draft RFP Section L	L4: Volume II – Gate Criteria Submission Instructions	Factor 1, Sub-factor 1.1	88	3263	The Government's edits to the DRFP removed the previous requirement for revenue reporting (previously Item d). Please confirm that revenue is not a required metric.	Revenue is not required as part of sub-factor 1.1.
1669	Draft RFP Section L	L4: Volume II – Gate Criteria Submission Instructions	Factor 1, Sub-factor 1.3	90	3339-3340	Please confirm that, consistent with Section C-4, a certification of ownership satisfies the documentation requirement in this clause.	Confirmed.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1670	Draft RFP Section L	L4: Volume II – Gate Criteria Submission Instructions	Factor 1, Sub-factor 1.6, ii	91	3396-3397	We request that the Government change DRFP Section L4, Subfactor 1 6, ii., Line 3396-3397, to state "To meet the criteria for ease of use, time to start provisioning must be less than 5 minutes based on the below criteria" and adjust the criteria as appropriate. CSPs facilitate marketplaces that include third-party software and services where provisioning times are dependent upon configurations that the CSP does not control. For example, if a third-party product uses templates that provision the CSPs' services on top of the core virtual machine (VM), this will extend the time it takes to fully provision the offering.	The requirement remains as stated; however, the Department is not prescribing which third-party product the Offeror uses for the demonstration videos indicated in sub-factor 1 6.
1671	Draft RFP Section L	L5: Volume III – Technical Criteria Submission Instructions	Factor 2, ii. 1	92	3498-3499	We suggest that this language be modified to acknowledge the fact that certain requirements of classified regions can make it undesirable or impossible to have exact parity with unclassified regions. We suggest adding the following: " offerings, unless divergence is required by other requirements of those regions, or as mutually acceptable to the Offeror and the Government."	The performance metrics about commercial parity have been clarified to measure based on ready for IV&V testing. Definitions for IV&V testing and commercial parity have been added to the Definitions Attachment.
1672	Draft RFP Section L	L5: Volume III – Technical Criteria Submission Instructions	Factor 2, iii. 7	94	3517-3518	With respect to cross-domain capability, does DoD intend this to mean S PRNet to JWICS and JWICS to SIPRNet? If so, will DoD provide the underlying technology to implement such a feature? If not, can DoD provide additional information regarding its cross-domain communication requirements?	The secure data transfer requirements have been clarified in the evaluation criteria. The Government does not intend to provide the Contractor a particular cross domain solution. The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1673	Draft RFP Section L	L5: Volume III – Technical Criteria Submission Instructions	Factor 3, iii	95	3551-3553	This requires that the proposed solution meet the definition of ruggedized as defined in Attachment 5, Section J. This is inconsistent with SOO 4 32 2, which requires MilSpec ruggedization only upon Government request. Given JEDI's focus on commercially available solutions, the Government will preserve flexibility in choice of offerings if solutions can be ruggedized to different standards (e g., non-MilSpec). If the Government agrees, we recommend removing Section L5, Factor 3, Section iii.1.a.	The Defintions Attachment has been updated for consistency. Ruggedized means that the system is specifically designed to meet or exceed M L-STD-810G standards to ensure reliable operations in harsh usage conditions. Whether the system needs to be tested and certified as meeting the standard is at the discretion of the Government.
1674	Draft RFP Section L	L5: Volume III – Technical Criteria Submission Instructions	Factor 3, iii. 2	95	3564-3572	The requirement for "static, modular, rapidly deployable data centers" is inconsistent with the JEDI scope of commercial cloud IaaS and PaaS. DoD has multiple, existing contract options for procuring modular, deployable data center solutions. In addition, those contracts include properly structured requirements and service level agreements that facilitate efficient sourcing and technical support. We respectfully request that the Government consider removing this requirement and the associated Pricing Scenario 5.	The requirement (and scenario) remains as stated, although clarified, in the final RFP.
1675	Draft RFP Section L	L6: Volume IV – Small Business Participation and Subcontracting Plan Instructions	Factor 8	97	3681	Please confirm that the Government intended CLINs x00104 and x00105.	The language has been updated to accurately reflect the CL N numbering in the final RFP.
1676	Draft RFP Section L	L8: Volume VI – Price Submission Instructions	Factor 10, 3	99	3751	Please confirm that the Government intended CLIN x00102 Classified IaaS and PaaS.	The language has been updated to accurately reflect the CL N numbering in the final RFP.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1677	Draft RFP Section L	L8: Volume VI – Price Submission Instructions	Factor 10, 3	99	3752	Please confirm that the Government intended CLIN x00103 Unclassified Cloud Support Package.	The language has been updated to accurately reflect the CL N numbering in the final RFP.
1678	Draft RFP Section L	L8: Volume VI – Price Submission Instructions	Factor 10, 3	99	3752	Please confirm that the Government intended CLIN x00104 Classified Cloud Support Package.	The language has been updated to accurately reflect the CL N numbering in the final RFP.
1679	Draft RFP Section L	L8: Volume VI – Price Submission Instructions	Factor 10, 3	99	3753-3755	The previous DRFP allowed links for a catalog. A catalog file will consist of hundreds of thousands of service line items. We request that DoD reconsider the option to link to a service catalog in lieu of a file.	A link alone is insufficient. The Government must have a clear and complete proposal, to include service pricing. Content on a website link could change at any time.
1681	Draft RFP Section L	L8: Volume VI – Price Submission Instructions	Factor 10, 3	99	3769-3770	Please confirm that the Government intended CLINs x00105 Portability Plan and x00106 Portability Test.	The language has been updated to accurately reflect the CL N numbering in the final RFP.
1683	Draft RFP Section M	M3: Evaluation Factors	Factor 8, (3)	105	Entirety	Because commercial cloud infrastructure services do not offer opportunities to subcontract, federal cloud infrastructure contracts generally do not incorporate small business plans. Can the Government confirm that—as with past performance evaluations, where a lack of past performance is evaluated neutrally—an Offeror's lack of experience with small business plans will be evaluated neutrally and not unfavorably?	The small business participation approach, which is now Factor 7 in the final RFP, no longer requires evidence of historical achievements of meeting small business goals. This Factor also now uses an adjectival rating scheme.
1684	Draft RFP Section M	M3: Evaluation Factors	Factor 10	106	4093	Please confirm that the Government intended CLINs x00105 and x00106.	The language has been updated to accurately reflect the CL N numbering in the final RFP.
1685	Draft RFP Section B	B	1	7	5	The description for CL N 100104 contemplates a bundled offering of services with differing levels of technical requirements. This CL N is firm fixed-price, and the description explicitly states that it is not a labor-hour based CLIN. The description, however, does not describe a specific task to be performed, as would be appropriate for a firm-fixed price CLIN, but instead describes a bundled set of variable, potential tasks and services. What is the Department's justification for utilizing a firm fixed-price CLIN in this situation?	This requirement has been clarified in the final RFP.
1686	Draft RFP Section H	H	5	18	288-323	Section H5 allows the Department to acquire new products and/or services from the contractor. The requirement, especially in the context of a ten-year contract, essentially locks in a single source for new capabilities not currently described in the contract. This approach can have multiple deleterious effects for the Department. It can limit access to new technologies, as some vendors may choose not to participate in the market under the framework of a locked-in vendor. In addition, it could place the government in the position of subsidizing its single provider's opportunity to impose anti-competitive terms and conditions on technology innovators seeking to supply new products, both under the program and in the commercial space. Maintaining multiple vendors will ensure access to innovative technology and provide price protections for the Department by allowing for competition for future procurements. In the previous Draft RFP comments, we asked how this Section is consistent with CICA, but we were not provided with a response to the question. We ask that the Department clarify how this requirement is consistent with CICA.	Your comment has been noted.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1687	Draft RFP Section H	H	7	19	345-362	Section H7 provides that security requirements are material to the contract. The Department notes that the contract and associated task orders may be terminated for default if the contractor fails to comply with security requirements. The nature of this requirement, however, evidences why the Department should utilize a multiple award framework. Having multiple contractors will provide redundancies in the event of failure, as well as multiple attack surfaces, which will increase difficulty for foes wishing to undermine DoD's activity in the cloud. Moreover, the use of multiple clouds already is common practice in the commercial market. These points were recognized recently by experts, including the former USDC3I and the current Chair of the Defense Science Board. See https://www.hudson.org/events/1542-merit-based-and-competitive-awarding-of-federal-it-services-public-policy-and-department-of-defense-cloud-computing42018. Furthermore, with a single awardee, in the event the Department needs to cancel a contract or order for security compliance issues, its options for alternative performance will be limited to non-existent, increasing its vulnerability in the face of potential threats. In contrast, multiple contract awards would provide the Department access to other vendors with alternative options to meet the Department's needs.	Your comment has been noted.
1688	Draft RFP Section L	L	4	91	3377-3401	Subfactor 1.6 requires the offeror to demonstrate an easy to use marketplace for offeror native services and third party services. What steps has the Department taken to prevent an organizational conflict of interest from arising in this marketplace? Is there any protection against potential pay to play schemes between the prime contractors and third party services? How will those markets operate and otherwise be rationalized with other e-commerce marketplaces, like FEDMALL, the GSA Schedules, and especially in connection with statutory compliance obligations, and any e-Commerce solutions currently under consideration in the government?	The scope of the third party marketplace offerings has been clarified in the SOO in the final RFP.
1689	Draft RFP Section M	M	1	100	3788-3805	(Part 1 of 2) The draft RFP contemplates a single award. 10 U.S.C. 2304a provides that implementing regulations must, "establish a preference for awarding, to the maximum extent practicable, multiple task or delivery order contracts." The regulations in FAR 16 504 provides that no task or delivery order contract exceeding $112 million (including options) may be awarded to a single source unless (1) the orders are so integrally related that only one source can provide the work, (2) the contract provides only for firm-fixed price orders where the product unit prices are established in the contract or the service are for specific tasks to be performed, (3) only one source is qualified and capable of performing the work at a reasonable price; or (4) it is necessary in the public interest to award the contract to a single source.	Your comment has been noted.
1690	Draft RFP Section M	M	1	100	3788-3805	(Part 2 of 2) In regards to (1), the draft RFP does not demonstrate that the orders are so integrally related that only one source can reasonably perform the work. In fact, the Department's cover memo undercuts any such argument, by stating that JEDI is "complementary" to other existing cloud initiatives. In regards to (2), although the CLINs are firm fixed price and not labor hour CL Ns, the services for which prices are established are not specific tasks to be performed. In regards to (3), the Department has stated publically that its market research has revealed that there are multiple sources capable of performing work. To date, the Department has not publicly released the written determination required by FAR 16.504 and 10 U.S.C. 2304a. In the interest of transparency and accountability, the determination should be made public. Will the Department release this determination?	While not required by acquisition law, the Department's rationale for single award has been released with the final RFP.
1691	Draft RFP Section M	M	1	100	3788-3805	Numerous comments on the draft RFP raised concerns about the Department's approach of utilizing a single contractor. It was disappointing to see that the Department's response was seldom more than, "Your comment has been noted." This response, along with the lack of the formal justification for a single award contract, is inconsistent with Deputy Secretary Shanahan's memorandum dated March 2, entitled "Communicating with Industry." The memo notes that "managing ...contracts requires the Department to engage in early, frequent, and clear communications with suppliers." Early, frequent, and clear communications are vital to a transparent and accountable acquisition process. As such, the Department should release its market analysis and business planning decisions for review by stakeholders and the oversight community.	Your comment has been noted. While not required by acquisition law, the Department's rationale for single award has been released with the final RFP.
1692	Draft RFP Section L	6	Small Business Subcontracting Plan	97	3688	RFP calls out a 20% allocation for Small Business Subcontracting Plan. The break out only shows 17%. Where do the last 3% go towards? Total Small Business - 20% - Small Disadvantaged Business - 5% - Women-Owned Small Business - 5% - HUBZone Small Business - 1% - Service-Disabled Veteran-Owned Small Business - 3% - Veteran-Owned Small Business - 3%	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation, which only applies to the Unclassified Cloud Support Package CLINs.
1693	Draft RFP Section L	6	Small Business Subcontracting Plan	97	3689	We are trying to determine why small business was not included in the list. Was the term Small Disadvantage Business suppose to be labeled Small Business?	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation, which only applies to the Unclassified Cloud Support Package CLINs.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1694	Draft SOO	4	4	6	206	Will the program office or DISA sponsor N PRNET, SIPRNET, JWICS circuit access to achieve the requirements of gaining accreditation and authorization requirements within 30 days of contract award for unclassified services; within 6 months of contract award for classified services at the Secret level; and within 9 months of contract award for classified services at the Top Secret/Sensitive Compartmented Information (TS/SCI) and Special Access Program (SAP) levels or is this contract intended to be awarded to CSPs that already have existing circuits and those CSP that do not have current network connecting cannot compete for this ward in order to meet the time requirements?	DoD will work with the awardee to sponsor the appropriate cryptography and circuit connections using bandwidth provided by the awardee.
1695	Draft SOO	4	4 8	7	240	Will DoD make available the DoD's provisioning tool, known as the Account Tracking and Automation Tool (AT-AT) in order for CSP's to build the appropriate APIs required to meet section 4.8 of the RFP stating that "the Offeror shall provide an API for the IaaS and PaaS offerings that is capable of creating, reading, updating, and deleting resources as identified below."	The Offeror must provide an existing API for functions identified in the SOO. The AT-AT system will use these APIs for interactions with the cloud environment.
1696	General					Given the important of avoiding lock-in, the government may want to expand the purview of this question beyond IaaS and PaaS to include management and automation tools. This is crucial to ensure that the DoD can use management and automation tools they have today to migrate and coordinate data and workloads in hybrid cloud environments.	Management of other departmental cloud offerings or data centers is outside the scope of this contract.
1697	General					Is there a requirement to provide any guarantee on API's for the IaaS or PaaS environments so that any changes do not disrupt applications that interact with the APIs in the case of an upgrade to the IaaS and PaaS layers?	The requirement has been clarified in the final RFP.
1698	General					Since the DoD will likely continue to operate traditional data centers, private clouds as well as utilizing future JEDI cloud services, Automation needs to cover the hybrid cloud use case. Just as the tactical edge is includes as a factor, the ability for automation tools to operate on-premise is important.	Management of other departmental cloud offerings or data centers is outside the scope of this contract.
1699	General					Is there a requirement to provide any guarantee on API's for the IaaS or PaaS environments so that any changes do not disrupt applications that interact with the APIs in the case of an upgrade to the IaaS and PaaS layers?	The requirement has been clarified in the final RFP.
1700	General					How will DoD ensure that customers can only deploy applications that are relevant to their requirements? For example, ensure that an Army customer cannot deploy an application that is exclusively paid for and used by the Navy?	The DoD's provisioning tool, known as the Account Tracking and Automation Tool (AT-AT), will manage user identity, access control, billing configuration, and security and configuration policy compliance. Identities and accounting codes associated with specific organizations will be linked.
1701	General					Will deployments be charged for applicable license/subscription fees?	The responsibilities for licensing terms and conditions for third party offerings in the marketplace are clarified in Section H in the RFP.
1702	General					Will there be an automated way to ensure IA/cyber authorization and compliance before applications are deployed?	The Department will explore innovative ways of accelerated accreditation in execution.
1703	General					How would new applications be added to the marketplace?	New applications in the marketplace would have to go through the process in the New Services clause in Section H of the contract before being added to the contract catalogs. Additional security authorizations may be required depending on the application. The performance metrics for commercial parity of marketplace offerings have been updated to account for the security authorization process.
1704	General					Assuming the application deployments are based on templates on not builds, who is responsible for keeping the templates in the marketplace up to date?	The SOO requires that the Offeror provide the ability to deploy third party marketplace offerings with baseline template configurations. The Offeror provides the ability, and the third party vendor would maintain the baseline template configurations.
1705	Draft RFP Section L	6	1	97	3680	Recent revisions in the second version of the RFP will exclude many qualified small businesses through the rigid application of specific percentages to individual categories of small business preferences. While the intent of these assigned percentages is noble, and clearly seeks to provide as broad an on-ramp to as many types of small business' as possible, the assignment of specific percentages is, in our view misguided, and will have exactly the opposite effect as that which is intended. In the first iteration of the draft RFP, small businesses were assigned 30% of the total work scope for the entire RFP- a broad and flexible allocation that allowed maximum flexibility to the prime contractor to meet the technical and programmatic needs of the warfighter. Draft #2 has made a significant and material impact to this requirement by reducing the total amount of the award available to small businesses to 20% and adding specific percentages to various small business preferences, such as HUBZone, small and disadvantaged, women-owned, service-disabled veteran-owned and veteran-owed. Whether or not these rigid percentages map against the very technical and precise technical skills actually available in the marketplace or would achieve a best value solution for the warfighter are not examined or justified. Such putatively exacting percentages, imposed as a requirement, would in our view actually curtail small business access by qualified small business' –all without necessarily meeting a best value solution for the DOD. We recommend that these individual percentages be discarded and that goals that allow the prime to adjust small business composition within the 20% be adopted instead of putative mandates.	The small business participation approach, which is now Factor 7 in the final RFP, has been substantially updated to allow for Offeror flexibility in proposing an achievable level of small business participation, which only applies to the Unclassified Cloud Support Package CLINs.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1706	Draft RFP Section L	6	1	97	3680	Line 3681 references CLINs X00401 and x00501 and we believe the intent was to reference CLINs x00301 and x00401 since x00501, addresses a Portability Plan	The CLIN references have been revised in the final RFP.
1707	Draft DD254	1	a	1		Will the Government help to facilitate the TS facility process for an application tha is pending for the Prime?	The Government will help facilitate a TS facility clearance for areas containing JEDI classified infrastructure or where Contractor staff will remotely administrate or manage the JEDI classified infrastructure or services.
1708	Draft DD254	1	a	1		Are all subcontractors required to have a TS facility clearance?	The Government will help facilitate a TS facility clearance for areas containing JEDI classified infrastructure or where Contractor staff will remotely administrate or manage the JEDI classified infrastructure or services. This includes Prime and Subcontractor facilities as needed.
1709	Draft DD254	10	0	2	0	Is the purpose of the DD254 in Block 10 to communicate to the contractor the potential scope of the security requirements associated with potential personnel on a task order basis?	The Prime Contractor is expected to have personnel or subcontractor personnel at contract award that can meet the requirements necessary to hold a security clearance meeting all requirements in Block 10. The Goverment will work with the Contractor to clear the personnel after contract award.
1710	Draft DD254	10	0	2	0	Does the govt intend for the contractor to have personnel cleared for all requirements specified in Block 10 of the DD254 prior to contract award?	The Prime Contractor is expected to have personnel or subcontractor personnel at contract award that can meet the requirements necessary to hold a security clearance meeting all requirements in Block 10. The Goverment will work with the Contractor to clear the personnel after contract award.
1711	Draft DD254	11	0	2	0	Is the purpose of the DD254 in Block 11 to communicate to the contractor the potential scope of the security requirements that may be designated on a particular task order?	Block 11 outlines the requirements and authorizations for the Contractor to meet the JEDI Cloud contract requirements. The Government will work with the Contractor after contract award to establish the required accounts, processes, and procedures to fulfill Block 11.
1712	Draft DD254	11	0	2	0	Does the govt intend for the contractor to have all requirements of Block 11 completed prior to contract award?	Block 11 outlines the requirements and authorizations for the Contractor to meet the JEDI Cloud contract requirements. The Government will work with the Contractor after contract award to establish the required accounts, processes, and procedures to fulfill Block 11.
1713	Draft DD254	10 & 11	0	2	0	If a separate room in a data center where classified/controlled information will be stored and processed is an accredited SC F and SAPF, will that meet all physical security requirements in Blocks 10 and 11?	A separate room in a data center with SC F and SAPF accreditation is likely to meet the requirements specified in the DD254.
1714	Draft DD254	0	0	0	0	When must the contractor have the SCIF built and accredited to meet the security requirements of the DD254?	The facility and infrastructure must be providing Secret services within 6 months, and Top Secret, SAP, and SCI within 9 months. The Contractor must work with the Government to obtain the necessary accreditations and authorizations so that the services are available within the required timelines.
1715	Draft DD254	0	0	0	0	What procedures has the Department developed to facilitate security clearance processing – including granting contractor personnel access to SAPs, CNWDI, NATO, and SCI compartments (e.g., TK, G, HCS) – for JEDI task orders?	Contractor personnel will be required to hold the clearances outlined in the DD254 but that does not mean that access to that information is guaranteed. The Contractor is expected to limit Contractor personnel access to Government data to the greatest extent possible. The clearance is required because the Goverment recognizes that some inadvertent access is inevitable, but will not tolerate intentional access without the Government directing that access.
1716	Draft DD254	0	0	0	0	How will any Department delay in processing and granting clearances and access be addressed?	The Government will take appropriate action to avoid and remediate, as necessary, any delays.
1717	Price Scenarios	Scenario 3		6	245	The pricing scenario discusses autonomous/disconnected operations of the edge and states "Once connected to the WAN, all processed data is securely transferred to object storage within the user's JEDI Cloud account. On a weekly basis the raw sensor data is transferred back to the user's JEDI Cloud account and stored in nearline storage...". Can you explain OSD's definition of transferred Specifically address how OSD's definition of tramsfer works for this scenario and what is the expected outcome once the transfer is completed: The Scenario is as follows: the video and audio data is ingested into the Edge Node where a real-time prediction analysis is performed" where "the results of the anlaysis must be accessible to, and consumable by, commanders in the field using a separate viewing application..." The real-time analysis will create new metadata and relationships that are stored in both SQL and Non-SQL databases and, as part of the metadata, includes the unique data identifier for the object which is stored in the tactical edge cloud object storage. At some point network connection is availale and transfer occurs. What information does OSD expect to be transferred? Is it acceptable to reun the algorithmic exploitation once the video/audio is transferred on the enterprise cloud to recreate the metadata? Does the unique object D assigned in the tactical edge need to be the same object ID available in the commercial cloud object storage after synchronization? For any workproducts created at the tactical edge during the network outage do these workproducts need to also reference the data objects stored in the cloud environment once tramsfer is completed? What type of auditing is required to demonstrate that all the data objects stored in the tactical cloud object store are successfully transferred to the cloud environment?	The final RFP includes clarification in the pricing scenario to address what should be synced.
1718	Price Scenarios	Scenario 3		6	254	The scenario seems to indicte that the model training is required to be performed in the edge device. Can OSD explain why the requirement is not to train on audio/video that has been transferred to the user's JEDI Cloud account and then deploy the model to the edge device for execution? This seems to be a more realistic operational concept.	The final RFP includes clarification in pricing scenario 3.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1719	Price Scenarios	Scenario 5		15	441	The scenario states "This ruggedized data center must be deliverable within 10 calendar days of request to a CONUS U.S. Military base " The 10 calendar day time indicates this is a critical capability to be deployed. Yet the requirement does not provide any stated requirement for accreditaion and connection to networks. We recommend that this requirement be updated to change the requirement to the following: "This ruggedized data center must be delivered, fully accredited under ICD-503 RMF at the unclass, secret and TS levels, within 10 calendar days of request to a CONUS U.S. Miliary base..." And then, "Once delivered to the OCONUS location the vendor has 10 days to Setup/Startup the ruggedized data center, connect to the networks and run the final accreditation testing to receive the ATO"	The pricing scenarios assume proper accreditation has occurred. Contractor travel to connect modular data centers is not required and should not be included in the proposal. The SOO in the final RFP has been updated to state that "All tactical edge capabilities must be remotely configurable and maintainable to the greatest extent possible." The Government will connect the modular data center to network and power as necessary.
1720	Price Scenarios	Section 5		15	451	For this pricing scenario we recommend that the 2000 virtual CPU cores be changed to 2000 physical cores. This is a clearer requirment for physical infrastructure and then DOD can allocate/carve up these 2000 physical cores as required by the applications.	All tactical edge devices are required to provide IaaS and PaaS capabilities. A definition for virtual CPU cores has been added to the pricing scenarios.
1721	Price Scenarios	Section 5		15	449	Sub point (a) states "Storage capacity for 100PB of information, spread across all forms of storage " In order for OSD to evaluate offerings we believe it is critical for OSD to break this 100PB out into file, block, hadoop and object storage capacities. Providing guidance like like 500TB of file, 500TB of block, 1PB of hadoop and 98PB of object would allow apples to apples comparison of the submitted pricing.	The level of specificity suggested by the commenter is not necessary.
1722	Price Scenarios	Section 5		15	435	The tactical edge typically requires additional support and services than what has been identified in this pricing requirement At a minimum the requirements should specifically include as part of the pricing: remote monitoring of all tactical edge devices, break/fix services for any failed component at any tactical edge device location, non-disruptive upgrades or replacements, IAVA and security updates to sustain accredited security posture and the ability to incorporate 3rd party technology components required to support specific mission requirements. With the market research OSD has performed, these are demonstrated capabilities currently being provided by commercial cloud service providers supporting the tactical edge.	The SOO in the final RFP has been updated to state that "All tactical edge capabilities must be remotely configurable and maintainable to the greatest extent possible." Tactical edge capabilities are required to meet all performance metrics in the SOO unless stated otherwise.
1723	Price Scenarios	Section 5		15	435	Sub point (a) states "Storage capacity for 100PB of information, spread across all forms of storage " Please confirm that this means sufficient capacity for storing 100PB of data and that the configuration and proposed price must account for all overhead required for the data durability and resiliency. In addition, to ensure OSD is able to evaluate "apples to apples" configurations please provide the minimum durability and resiliency required for each storage category. This is critical since an object solution that requires 3-copy replication for 100PB of storage to meet the durability and resiliency factor requires substantially more footprint, power and chilling that an object storage technology that only requires 25% overhead to meet the requirement. This should be a critical part of the evaluation since in the pricing scenario OSD has taken responsibility for transportation and power required for operations and cooling. Finally, please confirm that if the pricing approach proposed by the offer is a monthly cost/GB/month mechanism that this monthly cost/GB/month cost should be for the usable storage which includes all the overhead as part of the calculation. For instance, if the proposed solutions requires 3-copy replication to meet the durability and resiliency minimum then the monthly cost/GB/month price provided is, in essence, for 3 GB of raw storage capacity.	The language in the pricing scenario has been clarified
1724	Price Scenarios	Scenario 1		2	24 and 38	What components in the diagram on line 38 encompasses the web application referred to on line 24?	The language in the pricing scenario has been clarified.
1725	Price Scenarios	Scenarios 2 through 6		2, 6 - 19	38	Please provide diagrams for the scenarios 2-6 similar to the one provided on line 38 for scenario 1.	Diagrams are not necessary for any pricing scenarios. The diagram in pricing scenario 1 has been removed.
1726	Draft RFP Section C	C2 Program Managem ent	C2.c	14	157-158	The government has indicated that the program management requirement is not separately priced or billable. If the offeror's cost for program management is already included in our pricing for CL Ns 001 and CL Ns 002, can the offeror demonstrate the share of work a small business is performing PM activities in those CLINs and receive credit in the small business plan?	The final RFP adds a CL N for CCPO Program Management Support. The final RFP also clarifies the small business participation and reporting requirements.
1727	Price Scenarios	all				With the revisions to the JEDI price scenarios provided on May 31st, the references to pricing narratives previously identified in Section L of the second DRFP for Volume III Factors 2, 3, and 5 are no longer aligned. Will the government please provide updated draft instructions on how narratives for the revised pricing scenarios should be developed and in which volumes and factors they will be evaluated?	The final RFP includes updates to all relevant sections as necessary.
1728	Price Scenarios	all				Where in the draft pricing scenario template excel workbook does the government want to see PaaS pricing? For example, In the IaaS Compute tab, the government provides PaaS pricing. Should PaaS pricing go specifically in the features tab?	PaaS should be priced in the relevant worksheet in the Pricing Template (e.g., compute related capabilities should be in compute and storage related capabilities should be in storage).
1729	Price Scenarios	L	Pricing Scenaro 1	2	61	Could the government please describe the objective of the scenario to be in line with the SOO based approach of the RFP so the offer may propose a best value approach as opposed to a prescriptive approach? (For example, 6 node database cluster is a prescriptive requirement as opposed to a performance based objective or service level agreement.	The purpose of the SOO and the Pricing Scenarios are distinct. An appropriate level of specificity in the pricing scenarios is necessary to ensure offerors are proposing an approach and pricing against common requirements.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1730	Price Scenarios	L	Pricing Scenario 1	2	61	Is the database an IaaS or PaaS solution? If IaaS, please provide the performance specifications for the nodes. If PaaS, please provide the performance requirements (for example the HA SLA vs. a requirement for 6 nodes since PaaS will abstart that concern from the government).	The language in the pricing scenario has been clarified.
1731	Price Scenarios	L	Pricing Scenaro 1	3	64	Scenario 1 asks to price in a continuous 30 day increment. Scenario 1 also states that the database and static file store will grow by 0 2% monthly. This implies that the growth occurs after the 30 days which is outside the scope of the pricing. Should the growth of these items be priced? If so, for how many months should they be priced?	The language in the pricing scenario has been revised.
1732	Price Scenarios	L	Pricing Scenaro 1	3	68	Scenario 1 asks to price in a continuous 30 day increment. Scenario 1 also states that backups of the database are rotated to offline storage after a month. This implies that the rotation to offline storage occurs after the 30 days which is outside the scope of the pricing. Should the offline storage of these backups be priced? If so, for how many months should they be priced?	The language in the pricing scenario has been revised.
1733	Price Scenarios	L	Pricing Scenaro 2	7	162 - 166	Is there a peak traffic requirement that must be met with the Cloud/Garrison/Field ERP systems?	The rate of requests remains constant throughout the order period described by the pricing scenario. If Offerors are expected to price peak traffic it is specifically identified in the scenario (e. g., price scenario 1).
1734	Price Scenarios	L	Pricing Scenaro 2	7	180 - 182	Would the government please define "seats"? Are these equivalent to Licenses, and if so what licenses?	The language in the pricing scenario has been clarified.
1735	Price Scenarios	L	Pricing Scenario 3	9	264	Line 264 includes the concepts of both "real time" and "twice a day" are used in the same sentence. Will the government please clarify the requirement?	The language in the pricing scenario has been clarified.
1736	Price Scenarios	L	Pricing Scenario 3	9	249-250	The government mentions 20 devices on average and 40 deployed. Should the offerer price 20 or 40 devices?	The language in the pricing scenario has been clarified.
1737	Price Scenarios	L	Pricing Scenario 3	9	249-250	When the government states that 20 devices will be in operation on average does that mean that 240 GB of data be generated per hour when pricing this deployment?	The language in the pricing scenario has been clarified.
1738	Price Scenarios	L	Pricing Scenario 3	9	250, 277	RE: "After a 12 month period, and once each month thereafter, advanced data analysis..." Does the first analysis run include 11 months of data (because the 12th month is in process of being uploaded) or should it be assumed that the analysis will not occur until the 12th month of data is uploaded?	The language in the pricing scenario has been clarified.
1739	Price Scenarios	L	Pricing Scenario 3	9	250, 277	For pricing the access of data used in analysis for the sensor data will the analysis access the raw data or the processed data? (needed to calculate the cost of reading data as part of the analysis)	The language in the pricing scenario has been clarified.
1740	Price Scenarios	L	Pricing Scenario 3	9	274-275	Does "10 separate accounts" mean that the data analysis will occur across the output from 200 devices (10 systems with 20 average devices or is the 10 separate accounts using the data from one set of 20 devices? (this is needed to understand the pricing of data access)	The language in the pricing scenario has been clarified.
1741	Price Scenarios	L	Pricing Scenario 3	9	281-284	Could the government please describe the objective of the scenario to be in line with the SOO based approach of the RFP so the offer may propose a best value approach as opposed to a prescriptive approach? For example, highly available database.	The purpose of the SOO and the Pricing Scenarios are distinct. An appropriate level of specificity in the pricing scenarios is necessary to ensure offerors are proposing an approach and pricing against common requirements.
1742	Price Scenarios	L	Pricign Scenario 4	12	350-352	Should the price include the cost to gather and write the the log data or is that done outside the pricing scenario?	The language in the pricing scenario has been clarified.
1743	Price Scenarios	L	Pricing Scenario 4	12	381	What is the duration (in total hours) of the the 10 on-demand analysis jobs?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1744	Price Scenarios	L	Pricing Scenario 4	13	390	What is the duration (in total hours) of the the nightly analysis jobs?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1745	Price Scenarios	L	Pricing Scenario 5	15	451	This scenario does not discuss the type of workloads being run that will consume the 2000 virtual CPU cores and 200 virtual GPU cores. Line 436 states generically, "processing large quantities of data and regularly engages in various activities that need large, elastic computing power". What ratio of should be assumed for determining compute capacity in this scenario? Will the government please state a 4:1 ratio of vCPU to each physical CPU hyperthreaded core, and a 8:1 ratio of vGPU to each physical GPU core for this scenario.	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1746	Price Scenarios		all			The updated pricing scenarios appear to be inconsistent in asking for pricing information across unclassified and classified environments, option year, and total order numbers. In order to provide a TCO best value evaluation for all offerors, will the government consider being consistent and ask for similar unclassified and classified environments, option year, and total order numbers across all scenarios?	The pricing scenarios are a hypothetical sample set of the anticipated types of orders that users may place. Ordering is decentralized and will not follow any particular pattern. The pricing scenarios have not been updated as suggested by the commenter.
1747	Price Build-up Template					If the offeror is willing to offer more than one discount type to the government may the offeror add more than one row to the additional gross discount table in the pricing build up template.	The Price Template has been updated to allow for multiple discounts being proposed for a particular scenario in the PS(x) Discounts and Premiums worksheet.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1748	General Question	0	0	0	0	Section M of the RFP states that Price "will be evaluated based on a comprehensive review" and goes on to state the Government will calculate a Total Evaluated Price equal to the sum of the proposed prices for 1) Price Scenarios, 2) Portability CL Ns, and 3) Task Orders. Please confirm that the Government's price evaluation will be based only on the Total Evaluated Price and will not take into account proposed volume discounts and other discount structures that may be triggered at usage volumes greater than the usage volumes reflected in the Price Scenarios. Alternatively, in order to ensure an "apples to apples" evaluation of volume discounts proposed by Offerors, we request that the Government consider providing usage volume assumptions for each contract year upon which all Offerors can base proposed pricing for the Price Scenarios.	The Government is looking for the Offeror to propose its most favorable pricing and all applicable discounts. The final RFP clarifies how the Total Evaluated Price (TEP) will be calculated. Relative to discounts, the TEP only takes into account discounts applied to the Price Scenarios. Separate from the TEP, Offerors must submit all potential discounts, including any discounts beyond what are applied to the Price Scenarios, as part of Attachment J-3 Contractors Discounts, Premiums, and Fees.
1749	JEDI Cloud Industry and Gov't QA Price	0	0	0	0	In response to Question No. 1680, which suggested that DoD rely on the Contractor's online, commercial price catalog rather than incorporate a price catalog into the contract, DoD stated "Acquisition law constraints prevent the methodology the commenter is suggesting." Nothing in the Federal Acquisition Regulation or federal statute prohibits the Government from purchasing cloud services on commercial terms, including commercial pricing terms. Indeed, many federal customers purchase cloud services based on the CSP's online price catalog. Moreover, commercial CSP offerings enable Government customers to manage compliance with fiscal and appropriations law by, for example, setting alarms that would permit the Government to prevent spending more than any amount obligated or funded to a specific contract regardless of any service price change. Also note that CSPs typically decrease, rather than increase, service pricing; the Government should immediately benefit from price decreases in a Contractor's online service catalog rather than requiring a contract modification before benefitting from a price decrease. This approach would also reduce the contract administration burden on the Contractor and Government associated with routine CSP service catalog changes. We request that the Government reconsider allowing incorporation of commercial online service catalogs rather than incorporation of a contract price catalog.	The Offeror's proposed pricing must be fixed and certain; using online catalogs introduces ambiguity into the proposed prices because the Offeror's online pricing may change in the middle of the evaluation. Subsequent to award, any price adjustments cannot occur in the absence of contracting officer approval that the new price is fair and reasonable. Post-award the Government will strive to automate implementation of the Section H clauses to the greatest extent possible using the DoD's provisioning tool and other tools, as appropriate.
1750	General Question	0	0	0	0	Please confirm that performance requirements in the Price Scenarios that are not reflected elsewhere in the RFP documents (i.e., the RFP, SOO, or Cyber Security Plan) are not RFP requirements that an Offeror must meet in order to submit a responsive proposal and will not be contract performance requirements after award. For example, Price Scenario 5 now specifies a 10-calendar day delivery upon Government request, which is not currently reflected elsewhere in the DRFP documents.	The SOO has been updated to include performance metrics related to delivery of tactical edge devices. The Government did not intend to include performance requirements in the Price Scenarios that are not required by the contract. Any other instances of this occuring should be brought to the Government's attention during the solicitation question and answer process.
1751	Price Scenarios	1	a	1	8 - 9	Can the Government please clarify that "CONUS unclassified JEDI Cloud" includes FedRAMP High regions and services? In Draft 2 of the JEDI RFP Attachment 5, FedRAMP High regional services were defined as classified, which is inconsistent with common terminology.	The final RFP clarifies the assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1752	Price Scenarios	Price Scenario 1	N/A	3	85	The Government has unnecessarily restricted itself by requiring PKI cryptography. We request that the Government allow for any NIST-approved cryptography solution.	PKI cryptography is necessary for purposes of this scenario.
1753	Price Scenarios	Price Scenario 2	N/A	7	186-187	Can the Government please clarify what non-Government communications networks would be used that would enable access to the ERP system on the Secret network?	The specific communications network is not relevant. Assume internet transport is used in accordance with NSA's Commercial Solutions for Classified (CSfC) Suite B cryptography.
1754	Price Scenarios	Price Scenario 2	N/A	7	187	Can the Government please clarify what entity types are connected via the site-to-site VPN (e. g., field-to-field, field-to-garrison, field-to-cloud)?	The language in the pricing scenario has been clarified.
1755	Price Scenarios	Price Scenario 5	N/A	15	434	While we understand the mission requirement for a rapidly deployable data center referenced in Pricing Scenario 5, we strongly encourage the Government to reconsider inclusion of the portable modular data center requirement in the JEDI RFP. Pricing Scenario 5 makes clear that the portable modular data center requirement in the RFP—which must meet MILSTD, TEMPEST, and SCI requirements—is not a type of offering that is customarily offered for sale on the commercial market and is not part of any commercial cloud service. Indeed, DoD admitted that this requirement is not commercially available in its May 7 report to Congress. The Government can better meet its requirements for unique, highly customized, and portable modular data center capabilities in support of military operations through existing contract vehicles with systems integrators or through a specialized RFP focused on this requirement that will not artificially skew decision-making on commercial item cloud services. Inclusion of the portable modular data center requirement in this commercial item acquisition unnecessarily presents opportunities for solicitation protests.	JEDI Cloud must address the full range of military operations.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1756	Price Scenarios	Price Scenario 5	N/A	15	434	As currently structured, the portable modular data center requirement in Price Scenario 5 will disproportionately impact Offerors' Total Evaluated Price, skewing the RFP price evaluation in a manner inconsistent with JEDI's core IaaS/PaaS objectives. As written, Price Scenario 5 will make up a disproportionate amount of Offerors' Total Evaluated Price. Overweighting the portable modular data center pricing evaluation will mask the potential for much larger possible savings related to pricing for the actual cloud services that are the core driver for JEDI, which will result in higher overall costs for DoD. If the portable modular data center requirement remains in the final RFP, we respectfully request that the Government adjust the price evaluation scheme to emphasize core IaaS/PaaS services and deemphasize the portable modular data center requirement.	The other scenarios have been updated to run continuously for at least 12 months.
1757	Price Scenarios	Price Scenario 5	N/A	15-16	Entirety	DoD's revisions to Pricing Scenario 5 confirm that the RFP unreasonably elevates an Offeror's ability to offer an existing portable modular data center solution over an Offeror's ability to offer core IaaS/PaaS capabilities at all classification levels. The RFP provides for equal weighting of Offerors that propose existing Secret and Top Secret cloud capabilities and offerors that propose Secret and Top Secret cloud capabilities that will not be available until up to six and nine months after award. In contrast, the RFP penalizes Offerors that do not propose an existing portable modular data center solution by providing less weighting to solutions that are not currently available but are in production prior to March 2019 (and no weighting for solutions available after March 2019). In so doing, the RFP penalizes Offerors who have existing Secret and Top Secret cloud capabilities at award but do not have an existing portable modular data center solution available at award, while favoring Offerors that lack Secret or Top Secret cloud capabilities at award but have an existing portable modular data center solution at award. This is inconsistent with the core purpose of JEDI, which is IaaS/PaaS and not portable modular data center. We suggest that DoD revise Section M, Factor 3 of the RFP (p. 102, lines 3923-3925) to provide equal weighting to proposed portable modular data center solutions that are available at award and at any time up to nine months after award.	Tactical edge offerings are required for both unclassified and classified requirements. The proposed solution must be available and meet security requirements as specified in the Cyber Security Plan within 30 days of contract award for unclassified services, which includes unclassified tactical edge capabilities. Factor 3 has been revised to be consistent with this requirement.
1758	Price Scenarios	Price Scenario 6	N/A	17	494	Is the 500 GB of data reused or can it be disposed of after the initial process? If the data will be reused, it will require additional storage and associated costs over time.	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1759	Price Scenarios	Price Scenario 6	N/A	17	495-496	In previous Q&A responses related to price scenario solutions, the Government has replied, "The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution." With that in mind, we request that the Government allow Offerors to propose storage and analytics technologies that may not be categorized as data warehouse solutions but can meet the stated requirement more effectively and efficiently.	An appropriate level of specificity in the pricing scenarios is necessary to ensure offerors are proposing an approach and pricing against common requirements.
1760	Price Scenarios	Price Scenario 6	N/A	19	579-580	Can the Government please clarify whether the SAP implementation for Price Scenario 6g and 6h is at the Secret or Top Secret/SCI level?	The language in the pricing scenario has been clarified to assume the SAP implementation is running at the TS/SCI level.
1761	Price Scenarios	0	0	0	0	For All Pricing Scenarios, Will the Technology and Application Infrastructure, Logic, & Automation be provided to the Cloud Service Provider to host in IAAS and to migrate to some Cloud Native PAAS capabilities?	Migration services are outside the scope of JEDI Cloud.
1762	Price Scenarios	0	0	0	0	Factor 10 says that "The Government does not intend to engage in a cost analysis of all individual prices for the D/IQ." How does the Government intend to achieve fair and reasonable pricing for the unit prices of products and services offered by the JEDI contract awardee that are not represented in the Price Scenarios? "The fact that a price is included in a catalog does not, in and of itself, make it fair and reasonable." FAR 15.403-3(c). Fair and reasonable pricing could be established through task order competition by multiple CSPs. FAR 15.403-3(b)("When adequate price competition exists . . . generally no additional data are necessary to determine the reasonableness of price.").	The final RFP clarifies how price proposals will be evaluated.
1763	Price Scenarios	0	0	0	0	How does the Government intend to achieve fair and reasonable pricing for the unit prices of products and services offered by the JEDI contract awardee when the facts of the Price Scenarios are merely "for the purposes of this price scenario" (Q&A, ID Nos. 1482, 1483)? "The fact that a price is included in a catalog does not, in and of itself, make it fair and reasonable." FAR 15.403-3(c). Fair and reasonable pricing could be established through task order competition by multiple CSPs. FAR 15.403-3(b)("When adequate price competition exists . . . generally no additional data are necessary to determine the reasonableness of price.").	The final RFP clarifies how price proposals will be evaluated.
1764	Price Scenarios	0	0	0	0	Pricing discounts can be given both by unit, and through bottom line discounts against the total cost of the solution sought. For example, NASA SEWP and GSA Contractors are often motivated by competition to provide additional discounts against the total cost of solution. Without competition at the task order level, how does the Government intend to incentivize bottom line discounts that are divorced from the unit price? a. Without these bottom line discounts, how will the Government achieve fair and reasonable pricing?	The Price Scenarios and Price Template will allow Offerors to propose both unit and bottom line discounts. The Price Template has been revised to better accomodate different discount methodologies.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1765	Price Scenarios	0	0	0	0	Section H5 says that "When new services are offered, and not explicitly excluded by DoD, the Contractor shall update the services and corresponding prices in the online catalog(s) for this contract." How does the government intend to achieve fair and reasonable pricing (required by FAR 15.4) in future years (such as 2027) when the JEDI contract awardee will not compete against new services and products priced and developed by other CSPs? Fair and reasonable pricing could be established through task order competition by multiple CSPs.	While the question is outside the scope of the Price Scenarios and Price Template, the Government will incorporate new services in accordance with the contract clauses and the FAR.
1766	Price Scenarios	2	0	0	0	Price Scenario 2 describes an existing ERP system, and Question 1495 clarifies that the ERP "for price scenario 2 is a 'lift and shift' from a different hosting solution." The Government has repeatedly stated that migration is not included in this RFP. Is the cost of migration included in Price Scenario 2? How does the Government intend to achieve fair and reasonable pricing if the cost of migration is not being factored into Price Scenario 2 (and any other migrated application)?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1767	Price Scenarios	0	0	0	0	How do the Pricing Scenarios account for the potential impact of the slower performance of an application that was originally engineered on a different architecture (thus requiring greater usage of the JEDI contractor awardee's IaaS/PaaS services)?	The pricing scenarios describe the IaaS and PaaS required to run the applications in JEDI Cloud.
1768	Price Scenarios	0	0	0	0	How does the Government intend to level any inconsistent assumptions made and articulated by the Offerors?	The Government will evaluate proposals in accordance with the RFP and FAR.
1769	Price Scenarios	0	0	0	0	What level of cloud services are required to establish Isolated and logical enclaves in order to support the Secure Data Transfer scenarios?	This question is outside the scope of the Price Scenarios and Pricing Template. The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1770	Price Scenarios	1	0	0	0	Is the Web Application Stack expected to modernize with cloud native PAAS services or lift-and-shift "as is?"	The pricing scenario describes the IaaS and PaaS required to run the applications in JEDI Cloud.
1771	Price Scenarios	1	0	0	0	Scenario 1 stated repeatedly "do not price any costs associated with the migration of all of this data to JEDI Cloud". t did not explicitly state if costs associated with the lift & shift of the Web Application Stack should be priced. Please clarify costs for lift & shift.	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1772	Price Scenarios	1	0	2	31	What is the amount of data cached in CDN and frequency of refresh?	The language in the pricing scenario has been clarified.
1773	Price Scenarios	1	0	2	31	Is there a geographic distribution requirement and localization requirement for CDN content? (only in US/ other regions?)	The language in the pricing scenario has been clarified.
1774	Price Scenarios	1	0	2	31	Who provides the CDN? The CSP? Government? Application source that is moving in to JEDI?	The language in the pricing scenario has been clarified.
1775	Price Scenarios	1	0	2	31	Who provides the Load Balancer? The CSP? Government? Application source that is moving in to JEDI?	The language in the pricing scenario has been clarified.
1776	Price Scenarios	1	0	3	57	What is the retention duration of uploaded static files?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1777	Price Scenarios	1	0	3	61	Who provides the Database? The CSP? Government? Application source that is moving in to JEDI?	The language in the pricing scenario has been clarified.
1778	Price Scenarios	1	0	3	61	Are the database nodes read only? Or updatable? What is the latency tolerance for the nodes?	The exact configuration of the Government-managed database nodes running on JEDI Cloud IaaS will not affect pricing.
1779	Price Scenarios	1	0	3	66	What is the data retention requirement in database?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1780	Price Scenarios	1	0	3	68	What is the retention of offline backup retention requirement?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1781	Price Scenarios	1	0	3	75	Is the new result set appended each day or will it be refreshed completely? If it is appended, what is the retention requirement?	The language in the pricing scenario has been clarified.
1782	Price Scenarios	1	0	3	79	Does the static file store data require redundancy to a different region for disaster protection?	The language in the pricing scenario has been clarified.
1783	Price Scenarios	1	0	4	91	What is the retention requirement for logged activity?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1784	Price Scenarios	1	0	4	101	What is the scope of the support? (Run & Maintain or does it need to include SDLC)?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios. Maintaining the full scope of application development is not within scope of JEDI Cloud.
1785	Price Scenarios	1	0	4	101	Does the customer want to bring their existing licenses to Cloud?	The pricing scenarios have been clarified to specifiy whether the capability is provided as a JEDI Cloud offering or if the Offeror needs to price something.
1786	Price Scenarios	1	0	4	124	Are the users connecting from private network or over the internet?	Offerors should assume users are connecting over the internet unless explicitly stated otherwise.
1787	Price Scenarios	1	0	6	162	Does the solution require auditing capability? Such as CASB?	The pricing scenario states the capabilites required.
1788	Price Scenarios	1	0	7	177	What is the backup retention requirement?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1789	Price Scenarios	1	0	6	180	Does the ERP environment require frequent data refreshes?	The pricing scenario does not describe a requirement for any environment refreshes, so it should not be priced.
1790	Price Scenarios	1	0	7	208	Are all 30 field copies full sized or sub sets?	The pricing scenario states that all OCONUS and field ERP system deployments utilize a synced mirror of the CONUS database.
1791	Price Scenarios	1	0	7	215	What is the backup of 30 field copies and its retention?	The pricing scenario does not describe a requirement for any backup operations for the ERP system field deployments, so it should not be priced.
1792	Price Scenarios	1	0	7	325	Are the backups for remote environment kept locally?	The meaning of this question is unclear to the Government.
1793	Price Scenarios	1	0	8	223	What is the frequency of restores (ex. once per month)?	The pricing scenario decribes a single (one time) restoration.
1794	Price Scenarios	1	0	8	240	What is the frequency of restores (ex. once per month)?	The pricing scenario decribes a single (one time) restoration.
1795	Price Scenarios	1	0	9	270	What is the retention requirement for offline storage?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1796	Price Scenarios	1	0	10	292	What is the storage size of the tactical store?	The language in the pricing scenario has been clarified.
1797	Price Scenarios	1	0	11	331	What is the encryption mechanism required?	The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1798	Price Scenarios	1	0	13	394	What is the frequency of refresh of the environment?	The pricing scenario does not describe a requirement for any environment refreshes, so it should not be priced.
1799	Price Scenarios	1	0	14	426	What is the frequency of data refresh to on-premise?	The pricing scenario describes a single (one time) data export.
1800	Price Scenarios	1	0	15	465	What is the storage retention requirement?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1801	Price Scenarios	1	0	17	494	What is the storage retention requirement?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1802	Price Scenarios	1	0	18	533	What is the storage retention requirement?	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1803	Price Scenarios	1	0	19	547	What is the frequency of refreshing the environment?	The pricing scenario does not describe a requirement for any environment refreshes, so it should not be priced.
1804	Price Scenarios	2	0	0	0	Q&A ID 1495, Att 1 SOO stated on Page 5 – "but executing migration of systems to JEDI Cloud is outside of this SOO". Please confirm this is still Government's position on Scenarios 1 through 6.	The final RFP includes additional assumptions in the beginning of the pricing scenario attachment that apply to all scenarios.
1805	Price Scenarios	2	0	0	0	According to the description, there is 1 CONUS ERP system, 4 OCONUS ERP systems, and 30 Field ERP systems - a total of 35 ERP systems for this application. Will each of the 35 ERP systems be functioning as an independent system, or will each OCONUS system and Field system functions as a extension of the CONUS main ERP system? In other words, will there be synchronization between the CONUS main system and OCONUS system, between CONUS main system and Filed system? Please clarify.	The pricing scenario states that the database is a synced mirror.
1806	Price Scenarios	2	0	0	0	Will operation and maintenance of the OCONUS ERP systems and Filed ERP systems be performed by Government Personnel or Service Provider Personnel? Will O&M be performed in location or remotely?	Maintaining the full scope of application development is not within scope of JEDI Cloud. Operation and maintenance of the ERP application itself is irrelevant for the price scenario.
1807	Price Scenarios	2	0	0	0	What is the VPN bandwidth availability for the Field ERP systems?	The price scenario states that the bandwidth is 1 Gb/s.
1808	Price Scenarios	2	0	7	191	Does the ERP Technology and Application already do its own app and data synchronization from CONUS to tactical edge and external systems?	The language in the pricing scenario has been clarified.
1809	Price Scenarios	3	f	11	342	This section describes a SAP scenario which typically requires physical separation, however, the requirement states logical separation. Please confirm whether logical or physical is the correct separation.	The language in the pricing scenario has been clarified.
1810	Price Scenarios	5	N/A	15	443-444	How does DoD view this scenario as distinct from managed services and other managed IT resources?	The RFP describes DoD's requirements for JEDI Cloud.
1811	Price Scenarios	5	N/A	15	443-444	Given that cloud requires constant access to the network, while this data center must be able to operate in a disconnected state, how does DoD consider this cloud?	The RFP describes DoD's requirements for JEDI Cloud.
1812	Price Scenarios	5	N/A	15	443-444	Can DoD explain why what is essentially a managed data center, an existing class of service, is being included in an offering focused on public cloud computing?	The RFP describes DoD's requirements for JEDI Cloud.
1813	Price Scenarios	5	N/A	15	443-444	What mission need will drive the use of a local data center, as opposed to using network connectivity to link back to actual cloud data centers?	The RFP describes DoD's requirements for JEDI Cloud.

D #	Industry Submitted Information						Government Response
	Draft RFP #2 Document	Section	Subsection	Page #	Line #	Information Request (Question)	
1814	Price Scenarios	1		2	42-44	The requirement states "Each application node is hosted on a moderate performance compute instance (8 vCPUs and 32 GB of RAM)." Will the government allow multiple compute instances (VMs) to be hosted on physical server clusters with greater computing capacities as doing so is a standard practice in cloud computing?	Offerors are free to propose any solution that meets all of the requirements in the solicitation.
1815	Price Scenarios	1		3	50-51	Will the Government confirm that application components such as message queuing capability (comparable to Apache Kafka) will not be the responsibility of the bidder? t is assumed that these capabilities will be provided, installed, configured, and maintained by the application owner.	This pricing scenario explicitly includes a JEDI Cloud hosted and managed message queueing / event stream service.
1816	Price Scenarios	1		4	101-102	The stated scenario indicates that the first order will take place on October 7th 2019. However, the solicitation's Factor 3 - Tactical Edge section line 3925 states that "The Government will consider capabilities that will be in production by March 2019, but with lesser weight than existing solutions."Given that this order will be placed after March of 2019, is this evaluation guidance still relevant?	The order dates in the Price Scenarios are hypotheticals only and do not limit when orders will be placed in execution. Orders for tactical edge may be placed in advance of the dates reflected in the Price Scenario.
1817	Price Scenarios	5		15	437-438	This scenario requires "elastic computing power". Does the DoD desire this elasticity to be automated through the use of network, computing, and/or storage virtualization and cloud management and automation tools, or is the requirement simply to provide modular scalable hardware for the application hosted in Scenario 1 only?	Tactical edge capabilities are required to meet all performance metrics in the SOO unless stated otherwise, including elastic IaaS and PaaS offerings.
1818						Confirm if UPS and battery backup is required and for how long?	Assuming this question is specific to the modular data centers, Offerors should assume that power is handled by the Government. The Government will consider all possible solutions industry has to offer that will meet the requirements of the solicitation and will not be prescriptive by specifying a solution.
1819						Please confirm preferred level of fire protection inside the module. Assumed FM-200 fire suppression with smoke detection and Fire Alarm Control panel only.	Specific fire suppression capabilities are not required; the Department is looking for vendors to provide innovative products and services while following industry standards and best practices.
1820	General					The evaluation factor in the SSO indicates that OSD is currenlty looking for a single tactical edge solution. However, the scenarios described in Pricing Scenarios describe dramatically different workloads. For example the Price Scenario 2 Sample Classified COTS deployment + Tactical Edge is for enterprise ERP applications that require relational database and an OLTP architecture while the Price Scenario 3 Sample Tactical Edge + Peered Query is for data streaming HD video stream with advanced algorithmic exploitation, predictive analysis and playback. For scenario 2 the technology required is dramatically different than for Scenario 3. These scenaios and the others that JEDI will need to support reality leads to purpose-built, optimized tactical cloud solutions to support the intended workload. How does the stated evaluation approach acccount for this necessity? The optimization is critical to reduce the SWaP for the tactical cloud requiring smaller rack space, lower power and wieght for transportation which is a very real operational requirement given the cost of electrical production, cost of cooling, etc in harsh environments.	The evaluation criteria for tactical edge requires Offerors to propose at least one tactical edge capability from two different categories: one for portable devices and one for static modular rapidly deployable data centers. The Price Scenarios related to tactical edge invoke both categories.

EXHIBIT F

Attachment L-3

Joint Enterprise Defense Infrastructure (JEDI) Cloud

PERFORMANCE WORK STATEMENT (PWS)

Task Order 001: Cloud Computing Program Office (CCPO)
Program Management Support

Updated 26 July 2018

1. INTRODUCTION

1.1 DESCRIPTION OF SERVICES

The resultant Task Order (TO) is being executed under the Joint Enterprise Defense Infrastructure (JEDI) Cloud Indefinite Delivery/Indefinite Quantity (ID/IQ) contract. This TO is for the Contractor to provide the personnel, processes, and tools necessary to effectively manage JEDI Cloud within schedule, quality, and performance requirements. The Contractor shall establish and maintain a formal program management organization, which shall coordinate and interface with the Cloud Computing Program Office (CCPO). Interfacing with other offices within the Department of Defense (DoD) is expected; however, all interactions shall be coordinated through the CCPO.

The purpose of this PWS is to describe the performance-based services the JEDI Cloud Contractor is required to deliver under performance of this TO.

1.2 BACKGROUND

The CCPO is responsible for oversight and execution of rapid adoption of cloud services across DoD. CCPO's ultimate goal is to drive evolutionary change for the acquisition and management of Information Technology (IT) services in support of business and mission operations across the DoD by providing access to modern, enterprise-level cloud services. The CCPO will leverage public and commercial best-practices to champion the effort, minimizing barriers to accessing cloud while maintaining the highest integrity and ethical standards to preserve public confidence in the stewardship of Government resources.

CCPO is charged with managing the JEDI Cloud contract. Under this TO, the Contractor will deliver a program management capability that is complementary to CCPO. Highly coordinated program management capabilities between the Contractor and CCPO are critical to successful execution of the JEDI Cloud contract and to optimize the contract's capabilities in support of the DoD mission.

2. GENERAL REQUIREMENTS

2.1 PLACE AND PERIOD OF PERFORMANCE

Work under this TO shall be primarily performed at the Contractor's facilities for all tasks in Section 3 below; however, certain tasks as identified may require meetings in the National Capital Region (NCR), as defined by 10 USC § 2674(f)(2). The period of performance shall be for one 12-month base year and one 12-month option year, for a total of 24 months.

2.2 BUSINESS RELATIONS

The Contractor shall successfully integrate and coordinate all activities required to execute the requirements specified herein. The Contractor shall manage the timeliness, completeness, and quality of the contract deliverables. The services required under this TO are not inherently governmental. If the Contractor believes any actions constitute, or are perceived to constitute, personal services, it shall be the Contractor's responsibility to notify the JEDI Cloud Contracting Officer and Contracting Officer Representative (COR) immediately.

2.3 CONTRACT MANAGEMENT

The Contractor shall establish clear organizational lines of authority and responsibility to ensure effective management of the resources assigned to this requirement. The Contractor must maintain continuity between the operations at the CCPO and the Contractor's corporate offices. The Contractor shall establish processes and assign appropriate resources to effectively administer this contract. The Contractor shall respond to Government requests for contractual actions in a timely fashion. As required in Section C2 of the ID/IQ Contract, the Contractor shall have a single point of contact between the Government and Contractor personnel assigned to support this TO.

2.4 CONTRACTOR PERSONNEL, DISCIPLINES, AND SPECIALTIES

An integral part of successful performance under this TO is the production of quality performance requirements described in Section 3, and the responsiveness of Contractor personnel in the day-to-day output of work tasks. While the end product or deliverable is vital to the Contractor's successful performance, day-to-day oversight also includes client interaction and responsiveness. Accordingly, the Contractor is required to proactively maintain assigned tasks and be responsive to all entities with professional business dealings related to the assigned tasks.

The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

3. PERFORMANCE REQUIREMENTS (TASKS)

3.1 General. The Contractor shall perform all tasks described in Section C2 of the contract and all program management tasks in the ID/IQ contract PWS.

3.1.1 The Contractor shall provide a monthly Contract Progress Report (CDRL A001) for overall performance under the contract and a Task Order Progress Report (CDRL A015) for performance under TO 001. The Contract Progress Report shall include, but not be limited to:

a. Percentage of JEDI Cloud's unclassified usage compared to the Offeror's total utilization for the following metrics: 1) Network - Volume of commercial client traffic, in bytes, for public internet ingress and egress (at the logical cloud boundary outside of availability zones, *i.e.*, in and out of the CCO-controlled infrastructure) per month and aggregated for the duration of this task order; 2) Compute - Number of physical (not virtualized) compute (CPU and/or GPU) cores in use by application servers, which are defined as those physical servers that host the virtualized infrastructure and platform services used by end users (for example, a network router would not satisfy this definition of application server); and 3) Storage - Data, in bytes, for each of online, nearline, and offline averaged across the month.
b. Any reporting required to comply with the Monitoring Method applicable to the Performance Metrics Table in the ID/IQ contract PWS.
c. Reporting on GFP and GFI.
d. Reporting required by the Quality Control Plan (CDRL A010).
e. Summary usage metrics.
f. Areas of concern.

3.1.2 Kickoff. The Contractor shall arrange and execute a post-award kickoff within 15 days after contract award in the NCR using formal materials (CDRL A016). The location secured by the Contractor shall be within walking distance of a WMATA Metrorail station. This event may last up to three days and may need to accommodate up to 100 people with a variety of informational breakout sessions and working groups.

3.1.3 In-Process Reviews (IPRs). The Contractor shall arrange and execute, using formal materials (CDRL A016), quarterly IPRs. IPRs are attended in person in the NCR with the CCPO, unless otherwise waived by the CCPO Program Manager. Requirements of the IPR include, but are not limited, overall status update; identification of any upcoming changes in offerings and capabilities; specific recommendations on how to better optimize JEDI Cloud based on collected data with projections on how implementation of those recommendations would improve performance for that specific area; identification of areas where communication between the Contractor and CCPO could be improved with recommendations on how to improve it; status of and any issues around interfacing with the DoD's provisioning tool; identification of areas of concern with recommendations on how to mitigate risk; trends (overall service quality, utilization, efficiency, and cost); advising on the utilization of JEDI Cloud and how it aligns to the commercial trends and practices; and goal management to include recommendations and status of goals as identified by the Government (if applicable); discussion of any reports submitted to the CCPO required by the JEDI Cyber Security Plan during the last quarter, and any agenda items provided to the Contractor within 10 days before the scheduled IPR. The Contractor is responsible for providing an agenda, presentation materials, and meeting minutes (CDRL A016) at the Quarterly In-Process Reviews (IPRs).

3.1.4 Ad Hoc Reporting/White Papers. The Contractor shall work with the CCPO to satisfy ad hoc reporting needs. Delivering white papers (CDRL A012) to help inform CCPO decision-making around effective implementation of JEDI Cloud. This reporting is in addition to other reporting requirements mentioned herein.

3.1.5 Communication. The Contractor shall communicate with CCPO counterparts regularly, including but not limited to Program Manager, security, technical, user engagement, strategic communications, provisioning support, and contracts, and proactively raise issues that may affect contract performance.

3.2 Security. The Contractor shall perform all tasks and submit all security deliverables (CDRLs A003 and A011) necessary to provide unclassified and classified infrastructure and offerings in accordance with all security requirements and timeframes required in the contract. Achieving high quality security is an ongoing requirement that will require the Contractor's constant monitoring and oversight and proactive risk mitigation.

3.3 Small Business. Small business reporting for all TOs placed under the ID/IQ contract in accordance with all applicable FAR requirements and Attachment J-10 Small Business Participation Commitment Document (SBPCD) shall be submitted under TO 001 using CDRL A013. Small business participation reporting to the CCPO is required for all CLINs annually; however, small business participation goals are limited to those CLINs invoked in Attachment J-10, and is required annually.

3.4 Property Management. The Contractor shall provide management and reporting of Government Furnished Property for all TOs placed under the ID/IQ. The Contractor shall ensure its property management system is in compliance with FAR 52.245-1. In the event there are any changes to the pre-approved documentation provided at time of proposal submission, the Contractor shall provide updated documentation under CDRL A014, Technical Report. The Contractor shall also properly handle all Government Furnished Information for all TOs placed under the ID/IQ.

3.5 Ordering Guide. The Contractor shall deliver and maintain the Ordering Guide (CDRL A008) to provide users with information and procedures to effectively place TOs against the JEDI Cloud ID/IQ contract. The Ordering Guide will contain components developed by the Government, such as the process within the DoD provisioning tool, which is expected to constitute around 60% of the overall Ordering Guide. The Contractor will develop the content for the remainder of the Ordering Guide, which will start with when a JEDI Cloud user receives authorization to provision cloud offerings. The Contractor is responsible for reviewing the entire Ordering Guide, including the Government-developed sections, to validate that the Guide conveys a cohesive and easy-to-follow process for users. The Contractor shall address as part of the Guide any specific information that users need to understand to successfully order tactical edge, cloud support package, and online marketplace (including BYOL) offerings. The final Ordering Guide shall be delivered 15 days after the Government provides the inputs for the Government-developed sections to the Contractor.

3.6 Quality Control. The Contractor shall establish quality control methodologies to ensure that all services for all TOs are provided in accordance with the schedule, quality, and performance requirements in the contract. The Contractor shall submit a Quality Control Plan (QCP) (CDRL A010) that aligns to the Quality Assurance Surveillance Plan (QASP) attached to the contract at award. The Government will consider the proposed QCP of the successful awardee as a basis for developing the final Government QASP attached to the contract.

3.7 Delivering all CDRLs to the CCPO, and to the TO ordering activities as appropriate, as identified below in Section 4 IAW schedule, quality, and performance requirements.

4. DELIVERABLES

CDRL	Deliverable	Frequency / Date of First Submission	Medium/Format/ # of Copies	Submit To
A001	Contract Monthly Progress Report (CMPR)	Monthly	Electronic copy in Offeror's preferred format	CCPO
A002	Transition Out Plan	As required; Government has 15 calendar days to review, the revise and resubmit for approval five calendar days after receiving comments. Subsequent submissions required until the Plan is approved.	Electronic copy in Offeror's preferred format	CCPO
A003	Contract Security Management Plan	Within 30 days of contract award and then annually thereafter; updated annually or as required to reflect necessary changes.	Electronic copy in Offeror's preferred format	CCPO
A004	Technology Refresh Plan	Within 30 days after contract award and then semi-annually thereafter	Electronic copy in Offeror's preferred format using Microsoft Office	CCPO
A008	Contract Ordering Guide	Within 15 days of after Government developed sections provided; updated annually or as required to reflect necessary changes.	Electronic copy in Offeror's preferred format using Microsoft Office	CCPO
A009	Change Management Roadmap	Within 90 days after contract award and then annually thereafter	Electronic copy in Offeror's preferred format using Microsoft Office	CCPO

A010	Quality Control Plan	Within 30 days of contract award, then annually thereafter	Electronic copy in Offeror's preferred format using Microsoft Office	CCPO
A011	Security Authorization Package	Various depending classification level	Electronic copy in format acceptable to the FedRAMP process	CCPO
A012	Technical Report	As required	Electronic copy in Offeror's preferred format	CCPO
A013	Small Business Reporting	Annually after date of contract award	Electronic copy in Offeror's preferred format	CCPO
A015	Task Order Monthly Progress Report	As required	Electronic copy in Offeror's preferred format	CCPO
A016	Meeting Materials	Quarterly	Electronic copy in Offeror's preferred format	CCPO

Unless otherwise specified, the Government shall have fifteen business days to review and provide comments to all deliverables. Any deliverables that are not commented upon within that time frame are deemed approved. Offeror shall have fifteen business days to revise and resubmit any deliverables that the Government provides comments upon.

5. TASK ORDER ADMINISTRATION

5.1 CONTRACTING OFFICER'S REPRESENTATIVE

It is emphasized only the JEDI Cloud Contracting Officer has the authority to modify the terms of this TO; therefore, in no event will any understanding, agreement, modification, change order, or other matter deviating from the terms of the TO or the base ID/IQ contract between the Contractor and any other person be effective or binding on the Government. When/if, in the opinion of the Contractor, an effort outside the existing scope of the TO is requested, the Contractor shall promptly notify the JEDI Cloud Contracting Officer in writing. No action shall be taken by the Contractor unless the JEDI Cloud Contracting Officer has issued a modification.

5.2 GOVERNMENT FURNISHED PROPERTY

No Government Furnished Property is required for this TO. However, reporting of the GFP for all TOs placed under the ID/IQ is required under this TO.

5.3 SECURITY

All tasks must be conducted in full compliance with all security requirements of this contract, including the DD Form 254 attached to this TO.

EXHIBIT G

Joint Enterprise Defense Infrastructure (JEDI) Cloud

PERFORMANCE WORK STATEMENT (PWS)

Task Order 0002: Obligating the Indefinite Delivery/Indefinite Quantity (ID/IQ) Contract Minimum

Updated on 26 July 2018

1. PURPOSE

The purpose of this Task Order (TO) PWS is to obligate the difference between $1,000,000.00 and the amount obligated for the base year of TO 001 against the JEDI Cloud contract to satisfy the ID/IQ contract minimum guarantee in Section B2 of the ID/IQ contract. The Contractor will not deliver services or submit invoices under this TO. When future TOs are placed for services, the Government will administratively transfer the funds obligated under TO 002 to those task orders. Prior to the expiration of the base ordering period of the ID/IQ contract, the Government will ensure that the Contractor can invoice for all funds that are satisfying the contract minimum guarantee.

2. BACKGROUND

An ID/IQ contract must include a minimum purchase requirement. FAR § 16.504(a)(2). An ID/IQ contract without a minimum is considered illusory and unenforceable. *See e.g.*, *Torncello v. U.S.*, 681 F.2d 756 (1982). When a contract is executed, the Anti-Deficiency Act requires the Government to obligate funds in the amount of the obligation being incurred. *See* 31 U.S.C. § 1501. For an ID/IQ contract, the amount of the obligation being incurred is the contract minimum. The minimum must be obligated at contract execution. *See Matter of Bureau of Customs and Border Protection—Automated Commercial Environment Contract*, B-302358, Dec. 27, 2004.

EXHIBIT H

Attachment L-2

Joint Enterprise Defense Infrastructure (JEDI) Cloud
Price Scenarios
Updated 26 July 2018

1.0 For all scenarios:

a. Offerors should assume that the required solution is for an unclassified JEDI Cloud requirement in accordance with the SOO and JEDI Cloud Cyber Security Plan, unless the scenario explicitly states otherwise. For CONUS scenarios that do not specify an exact location, the Offeror shall price the most expensive CONUS "region" or "availability zone" proposed for JEDI Cloud.
b. Offerors should assume that all services and resources are utilized continuously, and that all storage and data is retained for the duration of the order, unless the scenario explicitly states otherwise.
c. Offerors should assume that the migration of any applications described into JEDI Cloud is an instantaneous operation that takes place on day 1 of the order unless explicitly stated otherwise; this migration of any applications is not to be priced.
d. Holidays, fiscal year end, and calendar year end have no effect on traffic patterns or scenario requirements. Leap years are not to be observed.
e. Offerors must propose a solution that is consistent with the solicitation, including all terms and conditions, requirements, and attachments, unless otherwise specified in the scenario.
f. No classified information is required, nor should it be provided, in any response.
g. If Cloud Support Package offerings are required by the scenario, the Offeror shall clearly identify the applicable tier of support and relevant category of services, including any service constraints. If meeting the specified requirement in the price scenario is dependent on ordering other Cloud Support Package offerings, then the Offeror shall also identify and price all dependent Cloud Support Package offerings.
h. The performance characteristics of virtual CPU (vCPU) and GPU cores in JEDI Cloud, including on tactical edge devices, must match the vendor's commercial cloud offering.
i. Assume all applications in all scenarios are fully deployed and running in a production environment.
j. Assume for all Ruggedized devices that the system does not need to be tested and certified as meeting the standard.

Price Scenario 1 Sample Unclassified Application Stack

A scalable application has the following traffic patterns in production:

- Averages 4,000 requests/min during normal business hours (Monday to Friday, 0900 – 1700 ET)
- Monday from 0900ET to 1200ET traffic jumps to 400,000 requests/min
- Tuesday through Friday from 0900ET to 1000ET traffic jumps to 20,000 requests/min
- Averages 500 requests/min outside the "normal business hours" specified above

A globally distributed JEDI Cloud CDN routes all incoming web requests to the application stack's load balancer. Static file requests are routed directly to the static file store by the CDN and account for 5% of all requests, averaging 40 KB in size. The CDN then caches the static file requested based on the expiration header information configured in the static file store (assume 30 days). All web requests are routed to a JEDI Cloud load balancer and average 10 KB in size. Load is then distributed evenly across healthy application servers with 10% of all requests resulting in an insert or update to the database. The system utilizes DNS Zone Hosting services offered by the JEDI Cloud vendor and averages 1000 DNS requests/hour.

The main application resides on multiple nodes that are evenly distributed among the available zones in the region, with a minimum of two nodes at all times. Each application node is hosted on a moderate performance compute instance (8 vCPUs and 32 GB of RAM) and can handle up to 500 requests per minute. During traffic spikes the number of required application instances is expected to grow dynamically using the auto-scaling capabilities available from the JEDI Cloud provider. Once a traffic spike has ended, the number of application nodes is expected to scale back down to appropriate baseline levels. All requests are authenticated using transport layer security (TLS).

Application activity will be pushed through a JEDI Cloud event stream (also known as a message queue) with functionality similar to Apache Kafka. Assume 90% of application requests result in events pushed to the queue, an average of 2 events per such requests, and each event is 200 KB in size. Eventually each event is read off the stream and results in an update or write to the database cluster. Users may also upload files to the application, where they will be stored in the static file store and retrieved dynamically according to an application specific access control mechanism. Additionally, the application will store short-term session information in a JEDI Cloud caching service. This session storage will start off at 1 GB in size on day 1 (do not price any costs associated with the migration of all of this data to JEDI Cloud), with 100 MB added each day and another 100 MB that expires each day.

The database cluster is hosted on six JEDI Cloud IaaS compute instances. The database contains 750 GB of data on day 1 (do not price any costs associated with the migration of all of this data

to JEDI Cloud). The nodes are evenly distributed among the available zones in the region, and each node requires a compute instance with 24 vCPUs, 256 GB of RAM, and 500 GB of normal SSD storage. Every minute, 500 MB of the 750 GB are updated. The data in the relational database will grow in size by 0.2% per month. Each day the reads from the application and analytics nodes total 1.5 TB in size. Automated snapshots are taken of the relational database daily using a JEDI Cloud service and rotated every 7 days. Weekly full database backups are created on Saturdays (starting the week the order is placed) and stored online for 4 weeks before being rotated to offline storage.

Four nightly analysis jobs are run on eight high performance RAM optimized compute instances requiring 32 vCPUs and 400GB of RAM each. Each instance should be powered down except for the two hours they run each night. These jobs will each read 700 GB of data from the static file store and 300 GB of data from the database cluster with no data preparation. Each job produces 5 GB of new results which are stored in a separate, redundant, multi-zone JEDI Cloud relational database service which requires 8 vCPU, 32 GB of RAM, and 300 GB of storage. All previous analysis job results are retained. This database service is separate from the database cluster mentioned in the previous paragraphs.

The static file store resides in a single region, will contain 1 TB of static files on day 1, and will grow as necessary (do not price any costs associated with the migration of all of this data to JEDI Cloud). Every minute, 700 MB of the 1 TB are updated with new content (each update request is 500 KB). The static file store content will grow 0.2% per month. Each day the reads by the application and analytic nodes total 2 TB in size (each read request averages 500 KB).

Of the files uploaded to the static file store, 33% require PKI encryption. Assume this application has one master key, which is managed by the JEDI Cloud provider. The application will request separate data keys based on that master for segments of its user population. Assume 5 new keys are created every day. The application will use these keys to encrypt 1000 files per day and decrypt 30,000 per day.

Every action that changes infrastructure configuration or alters infrastructure state is logged through a JEDI Cloud logging service (assume there are 20 such actions a day). Additionally, every data action taken for the managed data services is also logged through the same JEDI Cloud service. The infrastructure components running this application are continuously monitored through a JEDI Cloud service offering for performance degradation, which sends out an email alert if defined thresholds are exceeded for any infrastructure performance metrics. Additionally, there are 50 separate custom application metrics being monitored by this JEDI Cloud service, 25 of which will send out an email alert if defined thresholds are exceeded. In total, the JEDI Cloud service monitoring for this application sends 3 email notifications per day.

a. **Please price this scenario:** An order for a single application is placed on January 6, 2020, that meets the above technical requirements operating for 365 days continuously.

i. Please separately price all IaaS and PaaS offerings required to satisfy the above technical requirements for a single application.

ii. Please separately price services under the Cloud Support Package line item to support the application, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; access to detailed online training materials; and guidance on application and infrastructure architecture by phone using the lowest applicable tier.

b. **Please price this scenario:** The order is placed on June 7, 2021, for 50 applications total across 25 separate accounts, meeting the above technical requirements operating for 365 days continuously.

i. Please separately price all IaaS and PaaS offerings required to satisfy the above technical requirements for 50 applications across 25 accounts.

ii. Please separately price services under the Cloud Support Package line item to support the application, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; online instructor-led and on-demand online training for a total of 20 hours for 30 people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 40 hours.

c. **Please price this scenario:** The order is placed on June 3, 2024, for 1,000 applications total across 750 separate accounts meeting the above technical requirements operating for 365 days continuously.

i. Please separately price all IaaS and PaaS offerings required to satisfy the above technical requirements for 1000 applications across 750 accounts.

ii. Please separately price services under the Cloud Support Package line item to support the application, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; online instructor-led and on-demand online training for a total of 60 hours for 200 people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 80 hours.

d. **Please price this scenario:** The order is placed on June 7 2027, for 1,000 applications total across 750 separate accounts meeting the above technical requirements operating for 365 days continuously.

i. Please separately price all IaaS and PaaS offerings required to satisfy the above technical requirements for 1000 applications across 750 accounts.

ii. Please separately price services under the Cloud Support Package line item to support the application, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; online instructor-led and on-demand online training for a total of 60 hours for 200 people; and remote in-depth architectural

support for refactoring applications and configuring cloud infrastructure totaling 80 hours.

Price Scenario 2 Sample Classified COTS deployment + Tactical Edge

A Military Service utilizes an Enterprise Resource Planning (ERP) tool at the Secret level with a relational database included as part of the ERP to conduct supply, maintenance, and transportation services. The ERP has approximately 30,000 active user accounts across all commodities previously mentioned. This application is deployed to CONUS data centers, but has local, synced mirrors in garrison and aboard ship and in numerous austere environments, including a high likelihood of intermittent disconnected state. The ERP utilizes DNS Zone Hosting services offered by the cloud provider hosting the ERP. The hosted DNS service will receive 100 DNS requests per hour. The nature of this environment is such that a single user conducting maintenance can submit multiple service requests each hour.

Supply transactions consist of: generating reports, which vary in size but involve querying into the ERP's database, submitting requisitions for parts, obligating funds, and receiving requisitions.

Transportation transactions consist of managing shipments and movements of military equipment providing logistical support to an area. Units submit movement requests for each desired movement, identifying the requirement. The unit providing transportation then assigns organic equipment, forwards the request for any of the requests they cannot support to other units. Once a movement is completed a service request is completed for each vehicle used. Emails are regularly sent to the requesting and approving users confirming the transportation request status. Emails are sent from a hosted messaging service provided by the JEDI Cloud service provider. The ERP system sends a total of 500 messages per day.

Across all of the areas above combined, the main CONUS ERP system deployment handles a total of 1000 requests per minute with about three-quarters of those performing write operations in the database. Assume each OCONUS garrison ERP system deployment handles a total of 200 requests per minute and each field ERP system deployment handles a total of 50 requests per minute, regardless of the state of connectivity, with the same write operation ratio (three-quarters). Assume the size of each request for any ERP system deployment is 512 B and the associated response is 128 KB. Each request is received by a simple, JEDI Cloud provided load balancer which terminates SSL and then passes the request on to an available application node. The JEDI Cloud virtual machines that the ERP system is running on require 8 vCPUs and 32 GB of RAM per application node. Each virtual machine instance also requires 20 GB of simple Solid State Disk storage. There are 50 application nodes in the main CONUS ERP system deployment, 20 application nodes per OCONUS garrison ERP system deployment, and 10 application nodes per field ERP system deployment. Once per day, a snapshot of the entire provisioned block storage for each virtual machine is taken. These snapshots are kept for 7 days. Each ERP system deployment requires some JEDI Cloud virtual desktop working environments for use by the

Database Administrators (DBAs). These virtual desktops run Ubuntu, that requires the equivalent of 2 vCPUs and 16GB of RAM, have 10 GB of storage space, and are solely used for database access and tuning (they do not use or require any file sharing or additional systems or services). The main CONUS ERP system deployment requires 10 virtual desktops, each OCONUS garrison ERP system deployment requires 3 virtual desktops, and each field ERP system deployment requires 1 virtual desktop.

The ERP system is deployed in OCONUS garrisons using static, modular, rapidly deployable data centers. The ERP system is deployed in the field using ruggedized, portable edge devices that support disconnected operations and automatic resync of all data with the rest of the ERP system when possible.

To access the CONUS ERP system deployment while personnel are using non-government communications networks, a site-to-site virtual private network (VPN) tunnel to the JEDI Cloud must be utilized. 5 separate sites will each utilize a 1 Gigabit per second VPN connection 24 hours a day. The ERP will be expected to operate as both a completely self contained capability per specific performance characteristics as defined in this scenario and also be capable of re-integrating (on the fly), to all appropriate external systems that require data exchange with the ERP.

The database is currently 1 TB. A database dump will be uploaded to JEDI Cloud and then imported into the new JEDI Cloud database on day 1 of the order (network usage, data storage, and transaction fees associated with the transferring and importing of this data set should be priced; assume the uploaded data is deleted after the import is completed; as with all scenarios, do not price any migration support services). The database is expected to grow 0.5% per month. The highly available database cluster for the main CONUS ERP system deployment will be hosted in a JEDI Cloud service offering and requires 64 vCPUs and 400 GB of RAM. Each OCONUS ERP system deployment and field ERP system deployment has a local database that will use 2 compute nodes with 8 vCPUs, 64 GB of RAM, and 1TB of storage per node. Syncing data between the main JEDI Cloud database and the local databases is handled by the ERP system. Each OCONUS ERP system deployment writes 500 GB of data to JEDI Cloud once per week, downloading any other changes that have been made. Each field ERP system deployment writes 50 GB of data to JEDI Cloud once per week, downloading any other changes that have been made.

Every action that changes infrastructure configuration or alters infrastructure state is logged through a JEDI Cloud logging service, assuming there are 20 such actions a day. Additionally, every data action taken for the managed data services is logged through a JEDI Cloud service. Automated snapshots of the CONUS database occur daily and are kept online for 30 days before

rotation to offline storage along with weekly full backups taken every Saturday (starting the week the order is placed) that are rotated to offline after 30 days.

a. **Please price this scenario:** The order is placed on January 6, 2020, for the above technical requirements operating for 365 days continuously. In addition to the CONUS ERP system deployment, assume 4 garrison OCONUS ERP system deployments and 30 field ERP system deployments in ruggedized equipment.
    i. Please separately price all IaaS and PaaS offerings in JEDI Cloud, the modular data centers, and portable edge devices required to satisfy the above technical requirements.
    ii. Please price separately any non-consumption based fees or other charges associated with the number of modular data centers and portable edge devices required to meet the tactical edge storage and compute requirements for the specified OCONUS and field ERP system deployments.
    iii. Please separately price services under the Cloud Support Package line item to support all instances of the ERP system described in the pricing scenario, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; instructor-led and on-demand online training for a total of 20 hours for 30 people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 40 hours.
    iv. On January 30, 2020, a request is placed to retrieve a single offline backup of the database for use in forensic investigation. Assume the backup size is 950 GB. The retrieval shall be done as fast as possible, and the request is expedited.

b. **Please price this scenario:** The order is placed on June 7, 2027, for the above technical requirements operating for 365 days continuously. In addition to the CONUS ERP system deployment, assume 4 garrison OCONUS ERP system deployments and 30 field ERP system deployments in ruggedized equipment.
    i. Please separately price all IaaS and PaaS offerings in JEDI Cloud, the modular data centers, and portable edge devices required to satisfy the above technical requirements.
    ii. Please separately price services under the Cloud Support Package line item to support all instances of the ERP system described in the pricing scenario, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; instructor-led and on-demand online training for a total of 20 hours for 30 people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 40 hours.
    iii. On April 30, 2027, a request is placed to retrieve a single offline backup of the database for use in forensic investigation. Assume the backup size is 950 GB.

The retrieval shall be done as fast as possible, and the request is expedited.

Price Scenario 3 Sample Tactical Edge + Peered Query

A set of sensors on a government owned device captures 12 GB of High Definition Audio and Video data per hour. This data is collected 24 hours a day. There are 40 of these government devices deployed in the field for a specific operation. All of the sensor data from all of these government owned devices is streamed to a dedicated cluster of JEDI Cloud ruggedized portable edge devices in the field that has intermittent network access to a WAN. The cluster of one or more JEDI Cloud ruggedized portable edge devices must be able to store up to 2 weeks of sensor data.

The data must be processed daily by the portable edge devices regardless of connection; the devices will use JEDI Cloud PaaS offerings to conduct image recognition and audio analysis on the device itself. The analysis of video and audio will utilize a two stage, ensemble model. The first stage of the model will evaluate audio and video separately. All of the models used by the portable edge devices will be trained in JEDI Cloud and then synced to the devices before they are taken into the field. The first stage video model will be trained on 100,000 210 KB labeled 4k video frames. The audio model will be trained on 100,000 2 MB WAV files. The first stage models will classify and tag data for triage in which triaged data will be forwarded to the second stage of the ensemble model. The second model will take into account the output of both previous first stage models and will have been trained on a separate set of 100,000 labeled and paired audio and video files (assume this set also consists of 210 KB video frames and 2 MB WAV files).

Twice a day, an operator in the field will run a real-time prediction analysis on the portable edge devices using the ensemble model above. Results of the analysis must be accessible to, and consumable by, commanders in the field using a separate viewing application that the Offeror should not address as part of this scenario. Once connected to the WAN, all processed data is securely transferred to the user's JEDI Cloud account (*i.e.*, not on the portable device), including any meta-data and analysis results. On a weekly basis the raw sensor data is transferred back to the user's JEDI cloud account and stored in nearline storage for a period of 4 weeks before being rotated to offline storage. Offerors may assume that the weekly raw sensor data transfer occurs when a stable, high bandwidth connection is established between each portable device and JEDI Cloud.

Assume that the scenario described in the previous paragraphs is occurring for 10 separate operations simultaneously. 364 days after the initial order date, and once each month thereafter, advanced data analysis (referred to as the periodic advanced data analysis) using JEDI Cloud business intelligence PaaS offerings must be performed against a subset of the datasets across all 10 accounts. Each monthly analysis requires 32 vCPUs, 400 GB of RAM, and takes 36 hours to complete. There are 100 users with access to the analytics platform. As part of this cross-account

advanced data analysis, each of the 10 JEDI Cloud accounts also has a single JEDI Cloud relational database containing 10 TB of corroborating data. Each database is highly available, requires 32 vCPUs, and has 200 GB of RAM. The cross-account analysis must include data from these 10 traditional relationship databases (1 for each account, so 10 total). The cross-account analysis will be looking for specific patterns as well as anomalies. The total data to be analyzed is 10 PB (assume 2 PB of processed data, 500 TB of raw sensor data in online storage, and 7.5 PB of raw sensor data in offline storage that is loaded with a normal, non-expedited request). Predictions from this analysis are performed in batch (not real-time) and must be stored in another JEDI Cloud account (do not price any costs associated with the transferring or storing of the prediction results).

a. Please price this scenario: The order is placed on September 2, 2019, for the above technical requirements and operating for 15 months continuously where the classification level of the source data and the analysis results is Unclassified.

i. Please price separately the described number of tactical edge storage and compute devices.

ii. Please price separately all IaaS and PaaS offerings required to transmit and collect the data (across all of the accounts specified in the scenario).

iii. Please price separately all IaaS and PaaS offerings required to perform the advanced data analysis using cloud hosted, Offeror provided services across all of the accounts specified in the scenario.

iv. Please price separately all costs such that for every operation, there is an additional 10% identical spare portable tactical edge devices on-hand (minimum 2) at the base running the operation in case of failure (but that are not being utilized).

v. Identify and price any fee required upon return of the device to the vendor.

vi. Please price separately secure destruction of all classified storage media (applicable to paragraphs c, d, e, and f below in this price scenario) used upon mission termination in accordance with the Cyber Security Plan.

vii. Include any fees should the devices be entirely destroyed 364 days after the initial order is placed while in Government possession.

viii. Please separately price services under the Cloud Support Package line item to support the applications described in the pricing scenario for the initial 12 months only, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; instructor-led and on-demand online training for a total of 40 hours for 50 people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 80 hours.

ix. Identify any additional fee(s) if the Government retains the devices for an additional 12 months beyond the one year initial period of performance without

having placed another order. For purposes of this price scenario, assume that the ID/IQ option ordering period is exercised.

b. Please also price this scenario in accordance with the entirety of paragraph (a) above, but assume the order is placed on June 7, 2027.

c. Please also price this scenario in accordance with entirety of paragraph (a) above, but assume: the order is placed on June 7, 2021, the classification level of the source data and data analysis on the portable devices at the tactical edge is unclassified, a copy of all of the data transferred from all portable devices to any JEDI Cloud account is also simultaneously transferred to a single JEDI Cloud account operating at Secret classification, and the periodic advanced data analysis applications and results are classified at Secret.

d. Please also price this scenario in accordance with entirety of paragraph (a) above, but assume: the order is placed on September 2, 2024, the classification level of the source data is Secret, and all analysis applications and results are classified at Secret.

e. Please also price this scenario in accordance with entirety of paragraph (a) above, but assume: the order is placed on September 2, 2024, the classification level of the of the source data is Top Secret/SCI, and all analysis applications and results are classified at Top Secret/SCI.

f. Please also price this scenario in accordance with entirety of paragraph (a) above, but assume: the order is placed on July 5, 2027, the classification level of the entire program has been deemed a SAP at the TS/SCI level.

Price Scenario 4 Large Data Storage, Analysis, and Archiving

The following is an example of large data storage and follow up data analysis that retrieves and processes chunks of data from a large offline set.

A collection of systems across multiple accounts (assume 100) produces a large number of log entries every day. There are two different sources for the logs: (1) logs from the JEDI Cloud IaaS and PaaS offerings and (2) logs from the applications deployed in those accounts. Assume a total of 500 GB of logs in aggregate from all of the accounts each day. These log entries must be stored in a separate JEDI Cloud account (referred to as log collection account), which the individual account users have no access to (do not price the collecting, aggregating, or transferring of these log files into the log collection account). The team managing the log collection account only has read access to the storage. All data in the log collection account is rotated to nearline storage after 30 days, and then to offline storage after 90 days from creation and retained in perpetuity. Regular scans of these logs occur nightly and on-demand as described below.

The log collection and analysis team also has another JEDI Cloud account (referred to as the analysis account) for the analysis application used to analyze the data in the log collection account. The analysis application stack consists of a set of ten (10) high performance GPU nodes performing the analysis jobs (At Least 2 GPUs, 10 vCPUs, and 200GB of RAM per node), a set of four (4) moderate performance compute nodes hosting a clustered queueing and messaging system (At Least 8 vCPUs and 32GB of RAM per node), and a set of four (4) low performance compute nodes hosting a web-based graphical user interface (GUI) (At Least 1 vCPU and 1GB of RAM per node). The high performance GPU nodes each require an additional 50 GB of simple solid state disk (SSD) block storage to be provisioned. The web application is behind a JEDI Cloud load balancer that receives 100 requests per minute (512B request, 40KB response). The web application requires a single, low performance (but highly available) relational database that is provided as a JEDI Cloud PaaS offering (At Least 2 vCPU, 8 GB of RAM, and 100 GB of storage). Assume that there is already 2 PB of offline storage, 30 TB of nearline storage, and 15 TB of online storage in the log collection account on day 1 of the order (do not price any costs associated with the migration of all of this data to JEDI Cloud). For pricing purposes, “At Least” in this paragraph means that if the proposed JEDI Cloud service(s) do not identically match the specified minimum technical requirements, then the Offeror must propose the service(s) that satisfy those minimum technical requirements even if the level of service exceeds what is required by the scenario; in no event may an Offeror propose a service that does not meet minimum technical requirements).

Assume that 10 on-demand analysis jobs are run each week, with 4 pulling from online data, 3 from nearline data, and 3 from offline data. For each online on-demand analysis job assume the

average target dataset is 5 TB. For each nearline on-demand analysis job assume the average target dataset is 10 TB. For each offline on-demand analysis job assume the average target dataset is 50 TB and that offline data may be brought online with slow access (not expedited). In each case, the data is first copied in bulk to online storage (if necessary) and then analyzed. Any appropriate tags or markings identified by the analysis are applied to the original source data. The tags will be used in identifying that raw data at a later time for security review. Once the analysis is complete, if the data being analyzed was an online copy of nearline or offline data, the online copy is deleted. Nightly analysis jobs (assume 20 each night) run over online data only, but may process log files from any time during the 30 day rotational period in which data is kept online. Assume these nightly jobs process an average of 500 GB of online data each.

In total, analysis results consume 200 GB of storage per day on average. Analysis result data are tagged based on their source data, method of initiation, and other key markers and those tags are used in technical policy review and for billing purposes. Analysis results are saved in online storage for 45 days, nearline storage for another 90 days, and then archived into offline storage. Results stored offline are discarded after four (4) years. Assume the application has 4.5 TB of online result data, 4.5 TB of nearline result data, and 72 TB of offline result data on day 1 of the order (do not price any costs associated with the migration of all of this data to JEDI Cloud).

A user of the analysis application must be able to override the default lifecycle configuration set for the results such as setting alternate expiration dates and moving analysis results from one storage class to another. The application will execute API commands against the JEDI Cloud provider to accomplish this. Assume that users will transition 500 GB of storage from nearline to online each week and 200 GB of offline to online each week (not expedited).

a. **Please price this scenario:** The order is placed on January 6, 2020, for the above technical requirements operating for 365 days continuously.
    i. Please separately price all IaaS and PaaS offerings required to satisfy the above technical requirements.
    ii. Please separately price services under the Cloud Support Package line item to support the applications described in the pricing scenario, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; access to detailed online training materials; and guidance on application and infrastructure architecture by phone using the lowest applicable tier.

b. **Please also price paragraph (a) above,** but assuming that the order for paragraph (a) is placed on January 6, 2022.
c. **Please also price paragraph (a) above,** but assuming that the order for paragraph (a) is placed on January 6, 2025.

d. Please also price paragraph (a) above, but assuming that the order for paragraph (a) is placed on January 6, 2028.

e. Please price this scenario: The order is placed on October 31, 2023, for a complete exportation of all log data from the log collection account and all analysis results associated with the analysis application account described in this scenario. Assume log data totals of 15 TB of online data, 30 TB of nearline data, and 3 PB of offline data. Assume analysis result data totals of 5 TB of online data, 5 TB of nearline data, and 90 TB of offline data. Assume this request is not time-sensitive (no rush request). Assume the data must be transferred to an on-premise data storage solution provided by the Department that is capable of supporting the relevant data types in this scenario.

f. Please also price paragraph (c) above, but assuming that the order for paragraph (c) is placed on April 5, 2026.

g. **Please also price paragraph (c) above,** but assuming that the order for paragraph (c) is placed on April 5, 2028.

Pricing Scenario 5 Rapidly Deployed, Static Data Center

There is a forward operating base (FOB) that is processing large quantities of data and regularly engages in various activities that need large, elastic computing power. They need to rapidly get access to such computing power through static, modular, rapidly deployable data center(s) in short order.

This ruggedized data center solution must be delivered to a CONUS U.S. Military base within the number of days specified in performance metric 31 in Table 5.1 of the SOO from the order date. The ruggedized data center must be able to fit and be properly secured inside of a U.S. military cargo aircraft or ship and commercial shipping vessel. The data center should be able to operate fully (as specified below) in a fully disconnected state. Assume a solid pad for placement and clean power connections are provided by the FOB. The data center must be modular meaning that additional computing and storage resources can be added at a later date.

At minimum, each FOB site requires data center(s) to have:

(a) Usable storage capacity for 100 PB of data, spread across all forms of storage (objects, files, databases, file systems, etc.). All storage must be redundant (three copy minimum);
(b) Computing power of 2000 virtual CPU cores and 200 virtual GPU cores;
(c) Multiple data uplink options to include fiber optic, low and high bandwidth ethernet, and compatibility with standard satcom systems; and
(d) Implementation that meets CNSSAM TEMPEST/01-13: Red/Black Installation Guidance with regard to physical separation of environment where necessary.

a. Please price this scenario: The order is placed on November 4, 2019, for the above technical requirements operating for 365 days continuously for 10 FOB military deployment sites where there is an equal split of Unclassified, Secret, and Top Secret workloads at each site, including maintaining logical and physical isolation, as appropriate.

i. Please price separately all 10 FOB sites.
ii. In pricing the 10 FOB sites, for any consumption-based charges, assume a single copy of the application stack described in Pricing Scenario 1 is running in each modular data center throughout the duration of the order. Assume any nearline or offline storage remains online storage for the duration of the order.
iii. Please separately price services under the Cloud Support Package line item to support the data center deployments described in the pricing scenario, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; instructor-led and on-demand online training for a total of 60 hours for 200

people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 80 hours.

iv. Identify and price any fees required upon return of the data centers to the vendor.

v. Identify and price any fees for secure destruction of all classified storage media used upon mission termination in accordance with the Cyber Security Plan.

vi. Include any fees should the data centers be entirely destroyed at any point while in Government possession.

vii. Identify any additional fee(s) if the Government retains the data centers for an additional 5 months beyond the one year initial period of performance without having placed another order.

b. Please also price paragraph (a) above, but assuming that the order for paragraph (a) is placed on October 4, 2021.

c. **Please also price paragraph (a) above,** but assuming that the order for paragraph (a) is placed on October 7, 2024.

d. **Please also price paragraph (a) above,** but assuming that the order for paragraph (a) is placed on October 4, 2027.

Pricing Scenario 6 Containerized Data Analysis Framework

A military Service runs flight operations at a given base that produce logs on system function and maintenance needs. Separately, a maintenance system is used by the Service to enter reports on maintenance actions and scheduling. Each flight operation results in a large amount of data that is streamed after flight completion to a data warehouse hosted in JEDI Cloud. Maintenance records are stored in a separate system not hosted in JEDI Cloud. The Service will perform near real-time predictive analysis on both the flight data and maintenance records to determine future maintenance needs.

Each flight mission produces 500 GB of structured binary data per aircraft. Assume 20 flights per 24-hour period at the base. This data is streamed into the JEDI Cloud data warehouse directly post-flight. Assume the data warehouse storage backend has 1 PB of data in it on day 1 (do not price any costs associated with the migration of all of this data to JEDI Cloud). A total of 250 maintenance records are created per day at this base in the maintenance system (this system is not to be priced in this scenario). The maintenance system converts each record into a 500 KB structured record, which is sent via API call to a highly available JEDI Cloud serverless function, which requires 2.5GB of RAM to run. This serverless function parses the incoming data for validity and stores it in a highly available JEDI Cloud NoSQL document-based data store. Assume this NoSQL data store is 100 GB on day 1 (do not price any costs associated with the migration of all of this data to JEDI Cloud). The run time for each execution of this function is 1 second. In addition, to format validity of the maintenance record, the identity of the maintenance worker and their authorization to submit records for that aircraft is validated through a JEDI Cloud directory service. Assume there are a total of 10,000 identity objects and 1,000 other directory objects in the directory service for the base.

The flight operations system will push an event to a separate, highly available JEDI Cloud serverless function for each flight mission once that flight's operational data has been uploaded. The serverless function requires 512MB of RAM to run. This serverless endpoint will in turn add 1000 events to a message queue in a JEDI Cloud message service (each message is 50KB). The run time for each execution of this function is 500 milliseconds. Each message will be consumed by a data analysis application, which will start a data analysis job, which is hosted in JEDI Cloud. Each analysis job constructs and submits a query to the data warehouse service, which returns 1 GB of data. The results of the query are analyzed alongside the maintenance record data from the document store. The results of this analysis consume 5 MB of data and are stored in a highly available simple NoSQL key-value based data store. Assume this NoSQL data store is 500 MB on day 1. There are 10 such analysis applications in use within the overall system.

Each data analysis application stack is a collection of containers in a microservices architecture managed by a JEDI Cloud container orchestration service. Assume each application consists of 4

distinct microservices, hosted in 12 separate containers, and each container requires 2 vCPU, 2 GB of RAM, and 1 GB of storage. The application code for each microservice for each analysis job is version controlled in its own JEDI Cloud hosted code repository. On code commit to any master branch a set of tests are run using continuous integration hosted by JEDI Cloud. Each build for each of the code repositories requires that the build service utilize 2 vCPUs and 2 GB of RAM for 10 minutes. Assume a total of 10 builds are run per day. Following successful passing of the tests, a build artifact is produced and the resulting container is scheduled for zero-downtime redeployment. Assume 50 containers, that are each 1 GB in size, are generated and uploaded to a JEDI Cloud container registry every 7 days. The container registry contains 144 1-GB containers on day 1 (do not price any costs associated with the migration of all of this data to JEDI Cloud), and old containers are removed at the same rate that new containers are added (the total number remains constant).

A JEDI Cloud web application firewall is employed to protect the analysis applications from unwanted traffic. There are 30 custom rules in addition to any standard rules applied by the JEDI Cloud vendor. In total, the data analysis applications receive 100,000 requests per day between both valid and malicious actions. Automated security scans of the data analysis applications and data is performed daily, which includes threat identification, reporting, and real-time notification to the system owner.

a. **Please price this scenario:** The order is placed on January 6, 2020, for the above technical requirements operating for 365 days continuously where the classification level of the entire system is unclassified. This order is for operations on a single base.
    i. Please separately price all IaaS and PaaS offerings required to satisfy the above technical requirements.
    ii. Please separately price services under the Cloud Support Package line item to support all of the applications and services described in the pricing scenario, including at a minimum: 24x7 support by phone, web, and email; less than 1 hour response time for critical issues; less than 4 hours response time for moderate issues; instructor-led and on-demand online training for a total of 20 hours for 30 people; and remote in-depth architectural support for refactoring applications and configuring cloud infrastructure totaling 40 hours.
b. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on April 4, 2022, and the scenario is replicated at 100 bases.

c. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on September 5, 2022, and the system has been classified secret.

d. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on September 5, 2022, the system has been classified Secret, and the scenario is replicated at 100 bases.

e. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on July 1, 2024, and the system has been classified Top Secret / SCI.

f. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on July 1, 2024, the system has been classified Top Secret / SCI, and the scenario is replicated at 100 bases.

g. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on January 3, 2028, and the system has been classified as a SAP at the TS/SCI level.

h. **Please also price this scenario in accordance with entirety of paragraph (a) above,** but assume the order is placed on January 3, 2028, the system has been classified as a SAP at the TS/SCI level, and the scenario is replicated at ten (10) bases.

EXHIBIT I

[redacted]

Combined Congressional Report
45-Day Report to Congress on JEDI Cloud Computing Services Request for Proposal
&
60-Day Report to Congress on a Framework for all Department Entities to Acquire Cloud Computing Services

Key Points

- **Official Respondent:** Chief Management Officer
- **Official Recipients:** Chairs and Ranking Members of the House Armed Services Committee and the Senate Armed Services Committee as well as the Chairs and Ranking Members of the House and Senate Defense Appropriations Subcommittees
- **Due to Congress:** 7 May 2018
- **Sources:** Congressional report accompanying the *Consolidated Appropriations Act of 2018*
- **Background:** The Appropriations Act requires two reports and the HASC has requested a briefing that ask for significantly overlapping data points. The DoD has agreed to provide these reports to Congress simultaneously, at the 45-day mark. Below lists the requests and the recommended combined report structure.

Requesting Language

--Taken from Pages 88-89 of the legislative report attached to the Consolidated Appropriations Act 2018--

The Department, under the direction of the Deputy Secretary of Defense, created the Cloud Executive Steering Group to oversee this effort, referred to as the Joint Enterprise Defense Infrastructure (JEDI). This effort would be a tailored acquisition for commercial cloud services that could be a single award indefinite delivery/indefinite quantity contract for a period of up to ten years. There are concerns about the proposed duration of a single contract, questions about the best value for the taxpayer, and how to ensure the highest security is maintained.

Therefore, the Secretary of Defense is directed to provide a report to the congressional defense committees not later than 60 days after the enactment of this Act [due 5/22/2018] detailing a framework for all Department entities, to include combat support agencies, to acquire cloud computing services including standards, best practices, contract types, and exit strategies to ensure government flexibility as requirements evolve. The report should also include justification, to include cost considerations, for executing a single award contract rather than creating an infrastructure capable of storing and sharing data across multiple cloud computing service providers concurrently, to include data migration and middleware costs.

In addition, not later than 45 days after the enactment of this Act [report due on 5/7/2018], the Deputy Secretary of Defense is directed to provide a report on the JEDI cloud computing services contract request for proposals (RFP) to the congressional defense committees. The

[redacted]

report shall include the following: the amounts requested in the fiscal year 2018 and 2019 budget for this and all other cloud computing services acquisitions by appropriation; the fiscal year 2019 future years defense program levels for cloud computing services; identification and justification for acquisitions where "other transactional authorities" will be utilized; certification from the Department of Defense Chief Information Officer that each of the military Services, the combatant commands, Defense Information Systems Agency, and the Chief Information Officers of each of the Services have been consulted during the drafting of the RFP; provisions within the contract to ensure security is maintained over the period of the contract; and provisions for mitigation actions if the commercial entity were to provide services to or be acquired by a foreign entity or government.

1.0 Executive Summary

Secretary of Defense James N. Mattis recently told a gathering of soldiers, sailors, airmen and Marines that U.S. adversaries are making concentrated efforts to erode the nation's competitive edge. He added, "if we fail to adapt … at the speed of relevance, then our military forces and our Air Force will lose the very technical and tactical advantages we've enjoyed since World War II."

Technologies such as artificial intelligence (AI) and machine learning (ML) have the potential to fundamentally change the character of war. Modern computing capabilities can access, retrieve, manipulate, merge, analyze, and visualize data at machine speeds, providing substantial decision-making advantages on the battlefield. To maintain our military advantage, the Department of Defense (DoD) therefore requires an extensible and secure Cloud environment that spans the homeland to the global tactical edge, as well as the ability to rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance.

The JEDI Cloud is the initial step toward enterprise-wide adoption of foundational infrastructure and platform technologies available from commercial solutions. It does not encompass the full end-state of the Department's cloud computing vision. The DoD requires foundational technologies to capitalize on modern software, keep pace with commercial innovation and investment, and make use of artificial intelligence and machine learning capabilities at scale. JEDI Cloud will also provide opportunities to improve the Department's business functions through efficiencies gained and the ability to consolidate data centers and application software. It will reduce infrastructure investments and integration costs, which allow additional investments in military readiness and lethality.

The full and open competition for the JEDI Cloud contract will position DoD to get the best value in today's market of cloud computing capabilities to support warfighting and business requirements and grow capability as industry evolves. The initial two year base period of the JEDI Cloud contract allows for sufficient time to validate the Cloud's operational capabilities, DoD cloud migration processes, and the deployment of DoD enterprise-wide AI and ML applications. Option periods under the JEDI Cloud contract will be executed if doing so is the most advantageous method for fulfilling the DoD's requirements when considering market conditions at the time of option exercise. Regardless, DoD expects to maintain contracts with numerous cloud providers to access specialized capabilities not available under the JEDI Cloud contract, and to access Software as a Service (SaaS) capabilities.

JEDI Cloud must meet the Department's requirements of enabling warfighters to operate at mission speed, minimizing the introduction of security vulnerabilities, and achieving cost effectiveness at the speed of relevance.

Under current acquisition law, if the Department pursued multiple-award contracts for the JEDI Cloud, each individual task order would be competed, thus being paced by DoD acquisition

processes. That pace could prevent DoD from rapidly delivering new capabilities and improved effectiveness to the warfigther that enterprise-level cloud computing can enable. The Department anticipates working with Congress on additional contracts, industry growth plans, and broader whole of government deployment.

Several features of today's commercial cloud marketplace would likely impose additional costs and technical complexity on the Department in adopting enterprise-scale cloud technologies under a multiple-award contract. Requiring multiple vendors to provide cloud capabilities to the global tactical edge would require investment from each vendor to scale up their capabilities, adding expense without commensurate increase in capabilities. While security of data within clouds is largely standard and automatic, managing security and data accessibility between clouds currently requires manual configuration and therefore introduces potential security vulnerabilities, reduces accessibility, and adds cost. Maintaining inconsistent and non-standardized infrastructures and platform environments across classification levels complicates development and distribution of software applications, potentially adding delays and costs. Use of multiple clouds would inhibit pooling data in a single cloud (*i.e*., a "data lake"), limiting the effectiveness of machine learning.

The Department recognizes that the commercial cloud marketplace will continue to evolve. It is DoD's hope that cloud technology and offerings will become more interoperable and seamlessly integrated, enabling lower transaction costs and better inter-cloud security features, across multiple providers. DoD is best served by a robust, competitive and innovative technology industrial base. The Department will monitor the evolution of the marketplace, and work with Congress to be prepared with the acquisition laws and regulations needed to best achieve the DoD's missions.

Specific questions asked by Congress are addressed in the remainder of this report.

2.0 Why Cloud Matters: Warfighting Advantage

Battlefield advantage is driven by who has access to the best information that can be analyzed to inform decision making at the point and time of need. This advantage cannot be achieved at scale in the absence of an enterprise approach to adopting cloud technology. The 2018 National Defense Strategy (NDS) makes clear that the DoD needs a more lethal, resilient, and innovative Joint Force to preserve peace through strength and prevail in conflict when necessary. The NDS therefore prioritizes investments in cyber security, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Rapidly providing the DoD access to underlying foundational technologies, like cloud computing and data storage, on a global scale is critical to national defense and preparing the DoD to fight and win wars.

Towards these ends, the Joint Staff established the foundational requirements to guide DoD's migration to the cloud in the Joint Requirements Oversight Council Memorandum (JROCM) 135-17, *Joint Characteristics and Considerations for Accelerating to Cloud Architectures and*

[redacted]

Services, dated December 22, 2017. The JROCM stated that "efforts for accelerating to the cloud are 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." In particular, the JROCM stated that "cloud adoption should enable the capability to protect, detect, react, and restore at machine speed. Additionally, leveraging automated management and artificial intelligence will aid data-driven decision making." These warfighting requirements have driven every detail of the JEDI Cloud design.

Migration to cloud capabilities also supports the strategic direction of each Military Service. Each of the Services is pushing for greater interoperability on the battlefield to enable cross-domain warfighting. Substantial advantages for the Joint Force at the tactical edge can be delivered by leveraging rapidly evolving commercial technology that is common, globally accessible, resilient, and capable of operating in austere and connectivity-deprived environments. The ability to operate and collaborate in a common environment will lead to faster, better-informed decisions by operational commanders, and therefore vastly improve the lethality and efficacy of the military. Leveraging ML/AI at a tempo required to be relevant to warfighters, however, requires significant computing and data storage in a common environment. The DoD therefore must rapidly adopt the critical foundational technologies available in commercial cloud computing and storage, while eliminating considerable technical debt and security risk.

3.0 Terminology

There are a number of terms used in this report that can have a variety of meanings and are defined for purposes of this report below:

- *Modernization:* the act of taking existing software and rebuilding the architecture and software code in a modern way. As an example, an outdated Cobol-based financial billing system might be modernized and developed as a modular, containerized microservice architecture and web front end.
- *Migration:* the act of moving an application from one infrastructure or platform to another infrastructure or platform.
- *Infrastructure as a Service (IaaS)*: the equivalent of "bare metal" servers, networking, and data storage. It is the virtualization layer that allows the compute and storage resources from physical servers to be pooled and support many smaller, logical servers.
- *Platform as a Service (PaaS)*: the software, on top of an IaaS solution, that allows users to replicate, scale, host, and secure applications and data.
- *Software as a Service (SaaS)*: a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. Users have no control over the PaaS and IaaS underlying the software; it is sold as a complete technology stack.
- *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

[redacted]

[redacted]

is applied to a variety of different technologies (often without clarifying modifiers), but, for the purpose of this document, cloud refers to physical computing and storage resources pooled to provide virtual computing, storage, or higher-level services.

- *Commercial cloud*: means that a commercial cloud service provider is maintaining, operating, and managing the computing and storage resources that are being made available to customers. Depending on the contract, the commercial cloud service provider may be performing in commercial facilities or on premises in Government facilities. As examples, JEDI Cloud will be performed in commercial facilities whereas milCloud 2.0 is on premises in Government facilities.
- *Tactical edge*: means environments covering the full range of military operations, including, but not limited to, forces deployed in support of a Geographic Combatant Commander or applicable training exercises, on various platforms (e.g., dismounted infantry patrol, forward operating base, and aircraft carrier) and with the ability to operate in austere and connectivity-deprived environments.

4.0 Internal Investigation and Market Research

On September 13, 2017, the Deputy Secretary of Defense established an initiative to accelerate the adoption of cloud architectures and cloud services, focusing on commercial solutions in order to take advantage of the industry's ability to rapidly innovate. The memorandum establishing the initiative also identified the use of a tailored acquisition process to acquire modern enterprise cloud services that can support unclassified, secret, and top secret information. Since then, the DoD has conducted substantial internal investigation and market research to inform the acquisition process.

Numerous Focus Sessions were held with DoD Components, including the Under Secretary of Defense for Intelligence (USD(I)), DoD Chief Information Officer (CIO), Services, Joint Staff, United States Cyber Command (CYBERCOM), United States Transportation Command (TRANSCOM), Defense Logistics Agency (DLA), Defense Information Systems Agency (DISA), all four Service CIOs, and the National Security Agency (NSA). The meetings covered how each component was approaching adoption of cloud capabilities, how they intended to scale those capabilities, any perceived barriers to adoption, policy restrictions, security challenges, and potential lessons learned. There was a consistently expressed theme in the meetings that enterprise solutions are critical to achieving command and control and security in the cloud, coupled with economies of scale in terms of cost and maximizing cloud benefits such as advanced analytics, communication, and collaboration. All were concerned that DoD currently does not have the necessary workforce in place that can optimize cloud benefits.

DoD's extensive market research included a Request for Information (RFI) on October 30, 2017, interviewing major commercial firms that have adopted cloud technologies, conducting numerous meetings with cloud vendors, and examining best practices from the commercial industry. The DoD received 64 RFI responses, which indicated that:

[redacted]

- A cloud-based, virtualized computing and data infrastructure allows customer systems to easily scale, and provides better redundancy and failover than traditional data centers.
- Several companies have the existing infrastructure – in both scale and modernity of processes – to support many of DoD's mission requirements worldwide. However, some lead time will be required for any vendor to meet the full scale of DoD's classified and tactical edge requirements.
- Information security is a priority, and cloud providers are advancing rapidly in this space.
- Access to cloud resources through automation as much as possible is key to enabling an organization to rapidly adopt cloud infrastructure. Processes to automate include account provisioning, system configuration, security policy management, and billing.
- Operating austere and connectivity-deprived environments is commercially available to a degree, but still an evolving capability.
- Machine Learning and Artificial Intelligence systems are commercially available and continue to evolve at a rapid pace.
- The DoD's policies, particularly around security, limit its ability to fully realize the benefits of cloud technologies.

This internal and market research resulted in the establishment of the Cloud Computing Program Office (CCPO) on January 8, 2018, within the Office of the Chief Management Officer. CCPO will manage performance of the JEDI Cloud contract and has already issued two draft Requests for Proposals (RFPs). On March 7, 2018, DoD conducted a JEDI Cloud Industry Day with over 900 participants, at which speakers reiterated DoD's cloud requirements and commitment to conducting the JEDI Cloud acquisition through a full and open competition. On the same day, the DoD released its first draft RFP, to which 46 companies submitted more than 1,000 questions and comments. On April 16, 2018, DoD publicly responded to each of these questions and comments and issued its second draft RFP, to which it has received 394 additional questions and comments. This robust industry engagement through the draft solicitation process has helped industry understand DoD's requirements and helped DoD refine the solicitation.

5.0 DoD Framework

5.1 Acquiring and Using Cloud Computing Services

The DoD's adoption of cloud services to date has been mainly decentralized, with many organizations moving applications to the cloud, generally at small scale, with varying degrees of success. The DoD currently has multiple means of acquiring cloud computing capabilities, including in-house contracting activities, GovCloud, and GSA schedules. DISA also recently began offering milCloud 2.0 as an on-premises cloud solution. This decentralized activity has resulted in more than 500 individual cloud efforts, ranging from implemented cloud operations to those in the planning stage. While many of these separate initiatives help move individual user groups towards modernized software applications, they are reminiscent of DoD's current legacy information technology environment, which is not optimized for the 21st Century. The hundreds

of cloud initiatives have created numerous seams, incongruent baselines and additional layers of complexity for managing data and services at an enterprise level. Scattering DoD's data across a multitude of clouds further inhibits the ability to access and analyze critical data. As emphasized by DoD Components, enterprise efforts also are critical to achieving economies of scale and maximizing the benefits of pooled data and resources. The lack of a common environment for computing and data storage also will limit the effectiveness of ML/AI for warfighters.

Lessons learned from these cloud efforts helped inform DoD's enterprise cloud initiatives, including the JEDI Cloud, the Defense Enterprise Office Solution (DEOS), and DISA's milCloud 2.0. The JEDI Cloud will enable the DoD to efficiently and effectively conduct operations at strategic, operational, and tactical levels across classification levels and to the tactical edge. The commercial parity that will be delivered under the JEDI Cloud will allow users to easily provision assets, rapidly scale to meet demand, orchestrate cloud deployment, secure applications, and use ML and AI, all in a common environment. DEOS is a software-as-a-service (SaaS) cloud solution that will unify and modernize enterprise email, portal services, and enterprise collaboration tools. As a SaaS offering, DEOS will be complimentary to the IaaS and PaaS services in the JEDI Cloud. Similarly, milCloud 2.0 provides an immediate on-premises solution that will enable Components to reduce hosting costs relative to legacy data storage for applications that are ready for migration to the cloud. The DoD is working with user groups to prioritize which will move to milCloud 2.0, starting with Defense Agencies and Field Activities.

Once the JEDI Cloud contract is in place, the CCPO will initiate a series of proof-point validations that will trailblaze use of JEDI Cloud services and application migration. DoD partners for validation projects include the Navy, Marine Corps, TRANSCOM, and Defense Media Activity. The CCPO will lead development of a decentralized ordering tool that will allow DoD users to place task orders and rapidly gain access to centralized infrastructure and platform services at the appropriate classification level. The task order issuance process will be automated through a provisioning tool that will manage user identity, access control, billing configuration, and security and configuration policy compliance. During these operational validation activities, the DoD will ensure JEDI Cloud performs within the contracted standards and that we capture lessons learned and inform the activities of follow-on customers who move to the JEDI Cloud. Emphasis will be placed on understanding how to optimize the benefits of using cloud computing and storage infrastructure, particularly as it relates to data operationalization and advantaging the mission. For example, by moving Marine Corps logistics information and applications to JEDI Cloud, Marine Corps logistics will be able to incorporate modern technologies to optimize maintenance and distribution operations, generate analytics using multiple data sources to improve readiness and inform budget decisions, reduce the vulnerability of systems and applications, and set the conditions to allow for modern software development and delivery of new capabilities. To state this more simply, the Marine Corps will have better insight into all maintenance and logistics information and will be able to improve the readiness

to fight. Lessons learned from the validation activities for Marine Corps logistics will be synthesized and disseminated to other users.

While proof points are being validated, JEDI Cloud capabilities at higher classification levels and at the tactical edge will expand. While multiple commercial sources are capable of satisfying many of DoD's cloud requirements, establishing DoD's dedicated classified environment will take time, which is why the JEDI Cloud solicitation allows for a lead time of 6 months for Secret and 9 months for Top Secret and above. For tactical edge, certain industry sectors like oil and gas and university research have motivated vendors to develop commercial capabilities that can, at least to some degree, provide cloud computing and storage resources in austere and connectivity deprived environments. That said, because no other industry sector matches the scale and diversity of DoD's tactical edge needs, the JEDI Cloud solicitation allows for an initial capability that scales over time to support the full range of military operations.

Meanwhile, the DoD has already begun to reconcile, prioritize, and migrate the appropriate applications to the cloud. Many of the DoD's applications should be replaced with commercial software (including additional SaaS cloud offerings) or modernized. The Department is committed to consolidating or retiring legacy information technology. To facilitate such reconciliation, the DoD's Reform Management Group has begun work to inventory and prioritize applications for migration. Preliminary efforts focus on the 4th Estate and will soon be extended to the Services. The DoD will work with Congress as the software rationalization efforts continue.

5.2 Cloud Standards and Best Practices

Market research also indicated that initial migration to a single cloud is consistent with industry best practice. For example, a 2017 report by Gartner stated that "the impetus to "move to cloud" within many organizations is strong - in some cases, far stronger than the organization is truly ready to take on. The old adage of "crawl before you walk, walk before you run" applies." A separate Gartner report advices, "Much like the transition from mainframes to PCs, the transformation to cloud computing and hybrid IT architectures should be seen as a multiyear evolutionary process." The tremendous benefits of a centralized data lake were also widely discussed throughout market research and conversations. Consolidating most of the Department's innumerable data pools into a data lake can reshape both business and warfighting operations. As an example, today our munitions logistics are tracked separately by service and the total supply is manually tallied by analysts. Reallocation of those munitions is handled by phone calls and emails between logistics teams. The DoD relies on the skill and tireless effort of talented individuals to accomplish the mission today. If you look at major logistics, distribution, and supply corporations, they use a central data lake and predictive analytics to track supply levels which improves overall logistics efficiency and allows their personnel to focus on more complicated tasks. In addition to having a consolidated data lake, market research makes clear

that a well-articulated data strategy, including an architecture and data storage standards, is critical to realizing the benefits particularly with regards to ML and AI.

Consolidating Department data in a centralized data lake will significantly standardize the way DoD stores and tags data. This standardization will improve data security, accessibility, interoperability, portability, and usability. A centralized data lake will also allow the Department to use ML and AI without wasting computational power, storage, and time to aggregate and normalize data. The storage of data within the DoD on a robust cloud architecture provides for exploration and analysis which was previously beyond our capabilities.

The DoD can maximize the benefits of JEDI Cloud with applications optimized for cloud deployment. Applications should make extensive use of: web-interfaces, modern developer operations such as continuous integration and continuous deployment, architecture which separates application logic from data storage, and application programming interfaces which expose the data over secure, modern protocols. Additionally, the DoD must strive to make applications portable, whenever possible. Containerization -- the process of packaging all of the necessary platform and runtime information required for an application to run in a repeatable, code-defined process -- is critical to supporting portability. This is a best practice across industry and will enable application migration to other commercial clouds as needed.

6.0 JEDI Cloud Considerations

6.1 Contract Type

Given the state of the marketplace, cloud technology is generally a commercial item. When acquiring commercial items, Federal Acquisition Regulations (FAR) constrain available contract types to firm-fixed price (FFP), fixed-price contracts with economic price adjustment, or, under certain circumstances, time-and-materials or labor-hour contracts. The JEDI Cloud contract will be FFP that uses pre-negotiated catalogs resulting from the full and open competition. The JEDI Cloud contract will not use other transaction authorities (OTA) under 10 USC § 2371b.

Modernization and migration services, on the other hand, may not be limited to commercial item acquisitions depending on the degree of system customization and specialization for DoD. With non-commercial item acquisitions, other contract types, particularly cost reimbursement, become available. Cost reimbursement type contracts become more appropriate for complex application and migration issues so specialized that it is too difficult to predict the level of effort required and unreasonable to shift the risk of performance to the contractor.

6.2 Single Award Strategy

DoD is anticipating a single award indefinite-delivery, indefinite quantity (ID/IQ) contract for JEDI Cloud. The underlying documentation required by the Federal Acquisition Regulation to

support the single award ID/IQ approach is still under development within the Department. In no circumstance will the final solicitation be released until the underlying documents are executed.

The JEDI Cloud solicitation will include multiple mechanisms to reduce vendor lock and maximize DoD's flexibilities going forward. Because JEDI Cloud is an ID/IQ contract, DoD is only obligated to satisfy the contract minimum, which will be satisfied with the first task orders issued concurrent with contract award. Additionally, the initial base ordering period is limited to 2 years, which will allow for sufficient time to validate the operational capabilities of JEDI Cloud and the DoD enterprise-wide approach. Option periods under the JEDI Cloud contract will only be exercised if doing so is the most advantageous method for fulfilling the DoD's requirements when considering the market conditions at the time of option exercise. Even if an option period is exercised, DoD will not be obligated to place any orders, because the contract minimum would have already been satisfied. There are also portability requirements that enhance DoD's flexibilities as further described in the Exit Strategies section below. Finally, the contract reiterates that all Government data hosted by the contractor will remain the property of the Government and must be expeditiously extracted and returned, in accordance with security requirements, upon request.

The fact that Department will only ever be a fraction of the global cloud marketplace is to DoD's advantage. To capitalize on the benefits of this global competition, the JEDI Cloud contract will require ongoing commercial parity of technical offerings so long as the evolving capabilities comply with Department security requirements. There will also be contract clauses that ensure DoD continues to get the best pricing as global marketplace pressures drive prices down. In other words, the contract requires that the capabilities and prices delivered to DoD keep pace with commercial innovation.

The Department is best served by robust competition in an innovative industrial base. If the commercial cloud marketplace offerings evolve to become interoperable and seamlessly integrated, DoD could have the ability to meet warfighting and business requirements by employing a range of future contract and award types. However, based on the Department's extensive internal and external research, the planned approach will support rapid adoption of the commercial cloud technology at enterprise-scale, and allow the ability to change approaches in the future if conditions allow.

6.3 Contract Provisions for Security

The JEDI Cloud security requirements will be provided in the JEDI Cloud Cyber Security Plan, which will be approved by DoD CIO prior to releasing the final solicitation. It has been developed in close coordination with USD(I), DoD CIO, CYBERCOM, DISA, NSA, and others. The Cyber Security Plan establishes an exacting bar for outcomes but refrains from specificity in

implementation, so that the JEDI Cloud can capitalize on the rapid adaptation and innovation of the commercial sector.

Relative to Foreign Ownership, Control or Influence (FOCI), the contract includes provisions requiring compliance with the National Industrial Security Program, including the applicable FOCI requirements.

6.4 Exit Strategies

Exiting from any hosting environment is largely dependent on technical choices controlled by the application owner rather than the cloud provider. For instance, with JEDI Cloud, the DoD plans to make extensive use of containerization. Containers improve portability and allow for streamlined distribution and deployment of applications across cloud environments. Deciding to use containers, however, is a technical choice made by the application owner, not the cloud provider. Along similar lines, an application owner's use of data standards enhances portability.

Beyond application owner's technical choices, the JEDI Cloud contract will include a requirement for the contractor to provide a detailed portability plan (to include user instructions, processes, and procedures, such that any DoD customer can use these instructions to comprehensively migrate from JEDI Cloud to another environment) and regularly demonstrate portability of applications. The portability plan must also include an explanation evidencing the ability to demonstrate successful cleansing or destruction of all application components and an ability to prevent re-instantiation of any removed or destroyed application, capability (software or process), data, or information instances once removed from JEDI Cloud. Beyond a plan, the contractor must demonstrate migration of an application and data (provided by the Government for this purpose) from JEDI Cloud to a different hosting environment. The demonstration must validate the user instructions and evidence a reasonable ability to successfully migrate off of JEDI Cloud.

6.5 Certification on Coordination

The DoD CIO certifies that the militaryServices, COCOMs, DISA, and the CIOs of each military Service were consulted during the drafting of the RFP in the following manner:

- The DoD conducted Cloud Focus Sessions with all four military Service CIOs, DISA, and DLA in September and October 2017. These Focus Sessions aimed to inform the acquisition process.
- Throughout the JROC process, the entire user community, including COCOMS, had opportunities for inputs and feedback leading up to the ultimate signing of the JROCM 135-17 on December 22, 2017.

[redacted]

- The military Service CIOs and COCOMs reviewed the second draft of the solicitation package and provided comments, with particular focus on user requirements and security, to ensure the JEDI Cloud effort would be responsive to their requirements.

6.6 Cloud Computing in Wargaming and Military Exercises

Dating back to the early flight simulators of the 1920's, the U.S. military has stressed the importance of realism in training. This, in turn, has led to the development of increasingly effective operational and training military exercises that are based on the axiom that it is best to train as you fight. Wargaming and training systems of the near future therefore must incorporate big data, ML, and AI (1) to optimize the benefit of strategic simulations that feature advanced physical and socio-cultural-political factors/interactions in a realistic seeming world and (2) to emulate ML- and AI-driven challenges that our warfighters will face on the battlefield. The JEDI Cloud will provide the IaaS and PaaS compute and storage capabilities that such modern modeling, simulation, and wargaming software requires. Indeed, the Joint Staff and the Office of Cost Assessment and Program Evaluation are developing plans to apply ML and AI to strategic simulations, force management, and related activities. As JEDI Cloud capabilities become available, it is expected that similar efforts will be initiated for training and military exercises.

7.0 DoD Cloud Funding and Appropriations

Across numerous information technology systems and programs, the DoD's cloud computing budget request was $230 million in FY 2018 and $393 million for FY 2019 *(see attached, "DoD Budget for Cloud Computing"*). Total funding for cloud computing across the DoD's FY 2019-2023 Future Years Defense Program (FYDP) is currently projected at [redacted] (*see below, Table* "*DoD FY 2019-2023 Future Years Defense Program Cloud Computing*". To accelerate the migration of IT systems and data to the cloud the FY 2019 President's Budget request includes $160 million in FY 2019 and [redacted] in FY 2020 specifically for Cloud migration. Though neither the FY 2018 or FY 2019 President's Budget Requests for the DoD included a specific budget line item titled "JEDI Cloud". The DoD will prioritize reconciliation of applications, increased use of commercial software, and modernization of legacy applications.

[redacted]

Table 1

FY 2018 & FY 2019 DoD Budget for Cloud Computing

(dol ars in thousands)

Org	APPN	C	C itle	BA	PE	Budget Line Item	Budget Line Item itle	FY 2018	FY 2019
AIR FORCE	DWCF	93003	WCF, Air Force	20	0708202DF	N/A	N/A	27,958	23,631
AIR FORCE	DWCF	93003	WCF, Air Force		APPN TOTAL			27,958	23,631
AIR FORCE	Operat ons	3 00	O&M, Air Force	01	030511 F	1G-012A	Global C3I and Early Warning	87	90
AIR FORCE	Operat ons	3 00	O&M, Air Force	01	0308602F	1F-011Z	Base Support	185	185
AIR FORCE	Operat ons	3 00	O&M, Air Force	03	080 721F	31-031A	Oficer Acqu sition	-	3,21
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0308610F	50-0 2G	Other Servicewide Activ ties	-	5,183
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0901212F	50-0 2G	Other Servicewide Activ ties	99	99
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0901299F	50-0 2A	Administration	9,635	9,731
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0902 98F	50-0 2A	Administration	36	36
AIR FORCE	Operat ons	3 00	O&M, Air Force		APPN TOTAL			10,0 2	18,538
ARMY	Operat ons	2020	O&M, Army	01	0202218A	12-121	Force Readiness Operations Support	550	550
ARMY	Operat ons	2020	O&M, Army	01	020853 A	13-131	Base Operations Support	2,175	2,375
ARMY	Operat ons	2020	O&M, Army	01	0208853A	13-131	Base Operations Support	100	100
ARMY	Operat ons	2020	O&M, Army	0	0308610A	3- 32	Servcewide Communications	92	92
ARMY	Operat ons	2020	O&M, Army	0	0808716A	3- 3	Other Personnel Support	1,8 0	70
ARMY	Operat ons	2020	O&M, Army	0	0909398A	3- 35	Other Service Support	5	100
ARMY	Operat ons	2020	O&M, Army		APPN TOTAL			,802	3,687
DHRA	Operat ons	0100	O&M, DW	0	0901220SE	G- GT8	Defense Human Resources Activ ty	1,909	2,270
DHRA	Operations	0100	O&M, DW		APPN TOTAL			1,909	2,270
NAVY	DWCF	93002	WCF, Navy	08R	0605010DN	N/A	N/A	1, 3	,10
NAVY	DWCF	93002	WCF, Navy		APPN TOTAL			1, 3	,10
NAVY	Operations	1106	O&M, MC	03	0801712M	3C-3C1F	Recruiting and Advertising	10,26	10, 71
NAVY	Operations	1106	O&M, MC	03	080 751M	3B-3B3D	Profess onal Development Educat on	150	139
NAVY	Operations	1106	O&M, MC		APPN TOTAL			10, 1	10,610
NAVY	Operations	180	O&M, Navy	01	020 1 0N	1C-1C6C	Combat Support Forces	930	-
NAVY	Operations	180	O&M, Navy	01	020 11N	02-1B5B	Ship Depot Operations Support	1,219	1,2 0
NAVY	Operat ons	180	O&M, Navy	01	020 1 N	1C-1C6C	Combat Support Forces	2,087	2,123
NAVY	Operat ons	180	O&M, Navy	01	020 651N	02-1B1B	Mission and Other Ship Operat ons	150	71
NAVY	Operat ons	180	O&M, Navy	01	020 656N	02-1B2B	Ship Operations Support & Training	99	107
NAVY	Operat ons	180	O&M, Navy	01	0208550N	BS-BSIT	Enterprise Informat on	10,000	12,000
NAVY	Operat ons	180	O&M, Navy	01	0305013N	BS-BSIT	Enterprise Informat on	-	16,000
NAVY	Operat ons	180	O&M, Navy	01	0702207N	1D-1D D	Weapons Maintenance	270	270
NAVY	Operat ons	180	O&M, Navy	01	0702856N	1C-1C6C	Combat Support Forces	26	27
NAVY	Operat ons	180	O&M, Navy	01	0708012N	02-1B2B	Ship Operations Support & Training	-	757
NAVY	Operat ons	180	O&M, Navy	01	0708012N	1C-1C1C	Combat Communications	-	13
NAVY	Operat ons	180	O&M, Navy	01	0708012N	1C-1C6C	Combat Support Forces	26	26
NAVY	Operat ons	180	O&M, Navy	01	0708017N	02-1B2B	Ship Operations Support & Training	-	25
NAVY	Operat ons	180	O&M, Navy	01	0708017N	1C-1C6C	Combat Support Forces	7	7
NAVY	Operat ons	180	O&M, Navy	01	0808530N	01-1A2A	Fleet Air Training	5	5
NAVY	Operat ons	180	O&M, Navy	01	0901212N	1C-1CCY	Cyberspace Activities	11	16
NAVY	Operat ons	180	O&M, Navy	03	080 721N	3A-3A1J	Oficer Acqu sition	389	396
NAVY	Operat ons	180	O&M, Navy	0	090121 N	A- A1M	Administration	71	71
NAVY	Operat ons	180	O&M, Navy	0	0902398N	A- A1M	Administration	66	89
NAVY	Operat ons	180	O&M, Navy	0	0902 98N	A- A1M	Administration	30	30
NAVY	Operat ons	180	O&M, Navy			APPN TOTAL		15,826	33,713
NAVY	Operat ons	1806	O&M, Navy Res	01	0208550N	BS-BSIT	Enterprise Informat on	5,700	5,700
NAVY	Operat ons	1806	O&M, Navy Res			APPN TOTAL		5,700	5,700
NAVY	Procurement	1611	Shipbu ld&Conv, N	03	020 11N	01-30 1	LHA REPLACEMENT	390	-
NAVY	Procurement	1611	Shipbu ld&Conv, N	05	020 228N	01-5112	SHIP TO SHORE CONNECTOR	1,021	1,038
NAVY	Procurement	1611	Shipbu ld&Conv, N			APPN TOTAL		1, 11	1,038
NAVY	RDT&E	1319	RDT&E, Navy	0	060372 N	0829	ENERGY CONSERVATION (ADV)	320	320
NAVY	RDT&E	1319	RDT&E, Navy	05	060 567N	2 65	LHA(R) FLT Design and Total Ship Integration	-	397
NAVY	RDT&E	1319	RDT&E, Navy	06	0605898N	33 5	ONR Management Headquarters	1,000	1,000
NAVY	RDT&E	1319	RDT&E, Navy	07	0206629M	2938	Amphib ous Assau t Vehicle	299	308
NAVY	RDT&E	1319	RDT&E, Navy	07	0305208N	2227	D stributed Common Ground System (DCGS-N) Inc	1,000	1,500
NAVY	RDT&E	1319	RDT&E, Navy			APPN TOTAL		2,619	3,525
							Commercial Cloud otal	**82 115**	**106 816**
AIR FORCE	DWCF	93003	WCF, Air Force	0	0708211DF	N/A	N/A	1,006	873
AIR FORCE	DWCF	93003	WCF, Air Force	12	0708202DF	N/A	N/A	163	170
AIR FORCE	DWCF	93003	WCF, Air Force	20	0708211DF	N/A	N/A	68	81
AIR FORCE	DWCF	93003	WCF, Air Force			APPN TOTAL		1,637	1,52
AIR FORCE	Operat ons	3 00	O&M, Air Force	01	0101890F	20-015D	US STRATCOM	2 7	239
AIR FORCE	Operat ons	3 00	O&M, Air Force	01	03031 1F	1G-012C	Other Combat Ops Spt Programs	2,27	2,328
AIR FORCE	Operat ons	3 00	O&M, Air Force	01	0708550F	1F-011Z	Base Support	1 ,930	18,658
AIR FORCE	Operat ons	3 00	O&M, Air Force	03	080 721F	31-031A	Oficer Acqu sition	185	166
AIR FORCE	Operat ons	3 00	O&M, Air Force	03	080 731F	32-032A	Specia ized Ski l Training	183	187
AIR FORCE	Operat ons	3 00	O&M, Air Force	03	080 776F	32-032D	Training Support	3,762	3,832
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0702806F	2-0 1B	Technical Support Activ ties	2,536	2,257
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0708070F	2-0 1A	Log stics Operations	15	15
AIR FORCE	Operat ons	3 00	O&M, Air Force	0	0808716F	50-0 2A	Administration	275	283
AIR FORCE	Operat ons	3 00	O&M, Air Force	01	0305103F	1G-012D	Cyberspace Activities	-	66,000
						APPN TOTAL		2 , 07	93,965
AIR FORCE	RDT&E	3600	RDT&E, Air Force	0	0901 10F	6 3 83	CON-IT	500	77
						APPN TOTAL		500	77
ARMY	Operations	2020	O&M, Army	01	020201 A	12-121	Force Readiness Operations Support	380	380
ARMY	Operations	2020	O&M, Army	01	0202098A	13-133	Management and Operational Hq's	212	92
ARMY	Operations	2020	O&M, Army	01	0202218A	12-121	Force Readiness Operations Support	1,190	1,190
ARMY	Operations	2020	O&M, Army	01	020853	13-131	Base Operations Support	200	258
ARMY	Operations	2020	O&M, Army	01	0702207A	12-123	Land Forces Depot Maintenance	1,739	911
ARMY	Operations	2020	O&M, Army	03	080 721A	31-311	Oficer Acqu sition	5	6
ARMY	Operat ons	2020	O&M, Army	03	080 751A	32-323	Profess onal Development Educat on	85	87
ARMY	Operat ons	2020	O&M, Army	0	0303398A	3- 31	Administration	586	8 0
ARMY	Operat ons	2020	O&M, Army	0	0308610A	3- 32	Servcewide Communications	3,356	53, 83
ARMY	Operat ons	2020	O&M, Army	0	0708610A	2- 23	Log stic Support Activities	6,552	8,77
ARMY	Operat ons	2020	O&M, Army	0	0808716A	3- 3	Other Personnel Support	76	2,107
ARMY	Operat ons	2020	O&M, Army	0	0902398A	3- 31	Administration	99	1,0
						APPN TOTAL		15,568	69,172
ARMY	Operat ons	2065	O&M, ARNG	01	0522056A	13-131	Base Operations Support	989	638
ARMY	Operat ons	2065	O&M, ARNG			APPN TOTAL		989	638
ARMY	Procurement	2033	Proc of W&TCV, A	02	0211700A	20-3015GB 000	M2 50 CAL MACHINE GUN MODS	200	210
ARMY	Procurement	2033	Proc of W&TCV, A			APPN TOTAL		200	210
DCAA	Operat ons	0100	O&M, DW	0	0901516R	G- GT6	Defense Contract Audit Agency	1, 05	1, 32
DHRA	Operat ons	0100	O&M, DW	0	0901220SE	G- GT8	Defense Human Resources Activ ty	16,700	17,028
DHRA	Operat ons	0100	O&M, DW			APPN TOTAL		18,105	18, 60
DISA	DWCF	93005	WCF, Defense	17R	0303155DK	N/A	N/A	7,235	6, 0
DISA	DWCF	93005	WCF, Defense			APPN TOTAL		7,235	6, 0
DISA	Operat ons	0100	O&M, DW	0	03031 0K	G- GT9	Defense Information Systems Agency	10, 28	-
DISA	Operat ons	0100	O&M, DW	0	0305103K	G- GT9	Defense Information Systems Agency	2,836	-
DISA	Operat ons	0100	O&M, DW	0	0305013K	G- GT9	Defense Information Systems Agency	-	22,000
DISA	Operat ons	0100	O&M, DW			APPN TOTAL		13,26	22,000
NAVY	DWCF	93002	WCF, Navy	08R	0605010DN	N/A	N/A	60,520	61,777
NAVY	DWCF	93002	WCF, Navy			APPN TOTAL		60,520	61,777
NAVY	Operat ons	1106	O&M, MC	03	080 756M	3B-3B D	Training Support	23	28
NAVY	Operat ons	1106	O&M, MC	01	0305013M	BS-BSS1	Base Operating Support	-	6,000
NAVY	Operat ons	1106	O&M, MC			APPN TOTAL		23	6, 28
NAVY	Operat ons	180	O&M, Navy	01	020 221N	02-1B B	Ship Depot Maintenance	225	225
NAVY	Operat ons	180	O&M, Navy	01	020 230N	02-1B5B	Ship Depot Operations Support	90	90
NAVY	Operat ons	180	O&M, Navy	01	020 11N	02-1B5B	Ship Depot Operations Support	35	35
NAVY	Operat ons	180	O&M, Navy	01	0708012N	1D-1D D	Weapons Maintenance	107	107
NAVY	Operat ons	180	O&M, Navy	01	0708017N	02-1B2B	Ship Operations Support & Training	62	62
NAVY	Operat ons	180	O&M, Navy	01	0708017N	02-1B5B	Ship Depot Operations Support	208	211
NAVY	Operat ons	180	O&M, Navy	01	0708020N	02-1B5B	Ship Depot Operations Support	2,381	2, 0
NAVY	Operat ons	180	O&M, Navy	02	020 228N	2B-2B2G	Ship Activations/Inactivat ons	29	29
NAVY	Operat ons	180	O&M, Navy	02	0708017N	2B-2B2G	Ship Activations/Inactivat ons	18	19
NAVY	Operat ons	180	O&M, Navy	0	0708018N	B- B2N	P anning, Engineering and Design	162	162
NAVY	Operat ons	180	O&M, Navy	0	0901212N	A- A1M	Administration	3	9
NAVY	Operat ons	180	O&M, Navy			APPN TOTAL		3,679	3,712
NAVY	RDT&E	1319	RDT&E, Navy	02	0602750N	0000	UNDIST	600	600
NAVY	RDT&E	1319	RDT&E, Navy			APPN TOTAL		600	600
USD(AT&L)	Operat ons	0100	O&M, DW	0	0901388D8Z	G- GTN	Office of the Secretary of De ense	622	630
USD(AT&L)	Operat ons	0100	O&M, DW	0	0902198D8Z	G- GTN	Office of the Secretary of De ense	39	0
USD(AT&L)	Operat ons	0100	O&M, DW			APPN TOTAL		661	670
							Other Cloud otal	**147 788**	**286 370**
							otal Cloud Computing	**229 903**	**393 186**

Source: FY 2019 President's IT/Cyberspace Act vities Budget Request

[redacted]

Table 2

DoD FY 2019-2023 Future Years Defense Program Cloud Computing *(dollars in thousands)*						
Cloud Type	***FY 2019***	***FY 2020***	***FY 2021***	***FY 2022***	***FY 2023***	***FYDP***
Commercial Cloud	*106,816*	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Other Cloud	*286,370*	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total FYDP	***393,186***	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Note: Includes $160M in FY 2019 and [redacted] *in FY 2020 to accelerate the migration of IT systems and data to the cloud.*
Source: FY 2019 President's IT/Cyberspace Activities Budget Request

[redacted]

EXHIBIT J

DETERMINATION AND FINDINGS
FOR
AUTHORITY TO AWARD A TASK ORDER CONTRACT TO A SINGLE SOURCE

In accordance with Title 10, United States Code, Section 2304a(d)(3), I hereby make the following findings and determination concerning the award of an Indefinite Delivery/Indefinite Quantity (ID/IQ) contract to a single source to acquire a modern commercial enterprise cloud services solution for infrastructure as a service (IaaS) and platform as a service (PaaS) that can support all classification levels for the U.S. Department of Defense (DoD). This contracting action is known as the Joint Enterprise Defense Infrastructure (JEDI) Cloud acquisition.

FINDINGS

1. 10 U.S.C. § 2304a(d)(3)(B)(ii) prohibits DoD from awarding task or delivery order contracts exceeding $112 million (as adjusted for inflation under 41 U.S.C. § 1908), inclusive of all options, to a single source unless the head of the agency, as delegated to the senior procurement executive by 48 CFR 216.504 (c)(1)(ii)(D), determines in writing that the contract provides only for firm, fixed price (FFP) task orders or delivery orders for services for which prices are established in the contract for the specific tasks to be performed.

2. The Washington Headquarters Services (WHS), on behalf of the Cloud Computing Program Office (CCPO) in the Office of the Chief Management Officer (CMO), intends to award an ID/IQ contract for a modern commercial enterprise cloud services solution. To maintain our military advantage, the Deputy Secretary of Defense and Joint Staff established a requirement for an extensible and secure information environment that spans the homeland to the global tactical edge and can rapidly access computing and storage capacity to address warfighting challenges at the speed of relevance. DoD has recognized technologies such as artificial intelligence (AI) and machine learning (ML) are fundamentally changing the character of war. Leveraging AI and ML at scale and at a tempo relevant to warfighters requires significant computing and data storage in a common environment. Modern cloud computing capabilities can access, retrieve, manipulate, merge, analyze, and visualize data at machine speeds, providing substantial decision-making advantages on the battlefield. JEDI Cloud is an acquisition for foundational commercial cloud technologies that will enable warfighters to better execute a mission that is increasingly dependent on the exploitation of information.

3. The contract's ordering period will consist of a two-year base ordering period, a three-year option ordering period, another three-year option ordering period, and a final two-year option ordering period. The contract's maximum ordering period, if all options are exercised, will be 10 years with a maximum dollar value of $10 billion. The contract will be awarded pursuant to full and open competition.

4. The JEDI Cloud ID/IQ contract will provide for only FFP task orders for services for which prices are established in the contract for the specific tasks to be performed. Any discount methodologies proposed by the successful Offeror will be incorporated into the contract at award. For example, cloud vendors typically offer bulk discounts. Users will place FFP task orders based on the quantity and amount of cloud offerings (*i.e.*, IaaS, PaaS, and/or Cloud Support Package services) needed to meet the user's requirements, and reflective of any applicable discounts.

The contract line items (CLIN) are as follows.

CLIN	**Unit Price**
x*001 Unclassified IaaS and PaaS	By catalog
x002 Classified IaaS and PaaS	By catalog
x003 Unclassified Cloud Support Package	By catalog
x004 Classified Cloud Support Package	By catalog
x005 Portability Plan	As proposed
x006 Portability Test	As proposed
x007 CCPO PM Support	As proposed

* x001 represents the CLIN numbering system for each ordering period: 0001, 1001, 2001, 3001. This same numbering system is followed for all identified CLINs.

5. The CLINs for cloud offerings (*i.e.*, IaaS, PaaS, and Cloud Support Package) will be priced by catalogs resulting from the full and open competition, thus enabling competitive forces to drive all aspects of the FFP pricing. All catalogs will be incorporated at contract award and cover the full potential 10 years. Each offering in the catalog is provided "as a service", meaning that users will not be invoiced for labor-hours, time, or material; but rather a single, fixed unit price for delivery of that particular cloud service.

6. To allow the Department to take advantage of global marketplace competition on cloud pricing and new cloud services that emerge in the marketplace overtime, there are two pricing related contract Section H clauses that warrant mentioning. These two clauses allow the Department to access these advantages while still resulting in fixed unit price for delivery of all cloud services under the contract. To reflect the consistent downward trends in public cloud

catalog pricing based on commercial competition, the contract automatically lower DoD's prices when the contractor's public commercial prices are lowered. The lower unit price is fixed. Moreover, to achieve commercial parity over time, the contract contemplates adding new or improved cloud services to the contract. The new services clause requires contracting officer approval for the addition of new services and includes mechanisms to ensure that the fixed unit price for the new service cannot be higher than the price that is publicly-available in the commercial marketplace in the continental United States. This same clause requires that, if a service in the JEDI Cloud catalogs is eliminated from the Contractor's publicly-available commercial catalog, the Contractor shall offer replacement service(s) with substantially similar functionality as, and at a price no higher than, the service being eliminated. As with any other cloud offering, once the new service is added to the catalog, the unit price is fixed and cannot be changed without contracting officer approval.

7. The FFP CLINs that may only be ordered by the CCPO (*i.e.*, Portability Test, Portability Plan, and CCPO Program Management Support) will have fixed prices resulting from the full and open competition, and cover the full potential 10 years. As with the catalogs, the CCPO will not be invoiced for labor-hours, time, or material, but rather a single unit price for delivery of that service.

DETERMINATION

Based on the above findings, I hereby determine, pursuant to 10 U.S.C. § 2304a(d)(3)(B)(ii), that the ID/IQ contract for JEDI Cloud will provide only for FFP task orders for services for which prices are established in the contract for the specific tasks to be performed.

Ellen M Lord

JUL 19 2018

The Honorable Ellen Lord
Under Secretary of Defense
for Acquisition and Sustainment

Date

EXHIBIT K

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

JUL 26 2018

MEMORANDUM FOR JEDI CLOUD INDUSTRY PARTNERS

SUBJECT: JEDI Cloud Request for Proposals

Today the Department is releasing the final Request for Proposals (RFP) for the Joint Enterprise Defense Infrastructure (JEDI) Cloud Program, which is a pathfinder and a key component in the DoD's enterprise cloud environment strategy. Over the past year, stakeholders across the Department have engaged in a thoughtful, robust effort to build the JEDI Cloud Program, recognizing that we need to modernize quickly and to use a better approach to IT management. Working with technical experts across the Department, I have thoroughly reviewed this RFP and acquisition strategy. I am confident the JEDI Cloud RFP reflects the Department's unique and critical needs and employs the best standards of competitive pricing, innovation, and security. I am excited to be part of an initiative that will revolutionize how we fight and win wars.

Battlefield advantage is driven by who has access to the best information that can then be analyzed to inform decision making at the point and time of need. This advantage cannot be achieved at scale in the absence of an enterprise approach to adopting cloud technology. The 2018 National Defense Strategy (NDS) makes clear that DoD needs a more lethal, resilient, and innovative Joint Force to preserve peace through strength and prevail in conflict when necessary. The NDS therefore prioritizes investments in cyber security, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations. Rapidly providing DoD access to underlying foundational technologies, like cloud computing and data storage, on a global scale is critical to national defense.

The Department needs an IT environment that allows for data-driven decision making; enables DoD to take advantage of our applications and data resources; and achieves economies of scale across our vast enterprise. It is critical for the DoD to modernize quickly, while also changing the way it does business to keep that modernization moving forward at the speed of relevance. I firmly believe that the JEDI Cloud Program and the RFP being released today is the best strategy for the Department to meet its critical and urgent infrastructure needs. The JEDI Cloud Program is a pathfinder and a critical first step in the DoD's overall cloud environment that will provide an enterprise approach for obtaining general purpose infrastructure and platform services that can meet a majority of the Department's needs. We will take every advantage of learning from this effort to drive how DoD enables modern security practices and effective governance that still allows the flexibility to be innovative and keep pace with evolving technology. We also expect to learn a lot about the best ways to do enterprise architecture in a modern, relevant manner. With the diversity of DoD's mission, DoD will always have a multiple cloud environment, but we need to do better in applying an enterprise approach to that environment.

To successfully accomplish this, we are looking for an industry partner who will learn with us and help us find the best ways to bring foundational commercial capabilities to our warfighters. Industry has been incredibly active throughout this process, and I want to thank all of our partners for their incredible interest and participation. I expect you to continue to put your best foot forward with proposals and show us the best that industry has to offer. We're in this together!

Dana Deasy

EXHIBIT L

A HARVARD BUSINESS REVIEW ANALYTIC SERVICES REPORT

Harvard Business Review

HOW TO PLAN FOR A MULTI-CLOUD WORLD

sponsored by Google Cloud

SPONSOR'S PERSPECTIVE

When cloud computing first emerged, the question on many CIOs' minds was whether to adopt it at all. Eventually, the question became not whether, but when. Now it's which cloud tools and platforms to use and how to ensure they work together seamlessly and securely.

One of the great opportunities of cloud technology is the ability to combine and integrate different tools, services, and platforms. We are entering a future marked by openness and interoperability: According to recent research, 82 percent of enterprises have a hybrid cloud strategy, running applications in an average of 1.5 public clouds and 1.7 private clouds; and IDC predicts increasing adoption of hybrid cloud architectures.

That's good news for businesses. Open architectures protect companies from vendor lock in, add critical redundancies, and enable IT leaders to tap the best solutions to meet their unique business needs without arbitrary constraints that impede progress.

Google Cloud was built to help companies succeed in this open, multi cloud world. Our commitment to openness ensures seamless user experiences across multiple environments and empowers our customers to choose the right tools and platforms to meet their business needs.

Openness enables businesses to tap innovation without restriction, and it's been part of Google's DNA since the beginning. We've released more than 20 million lines of code in more than 900 projects including Chromium (the project behind the Chrome browser and operating system), TensorFlow (our open source machine learning library), and our popular container management system Kubernetes. We have a track record of incubating today's most compelling innovations from MapReduce (which directly inspired Hadoop) to our early efforts that enabled today's revolution in containers. With each breakthrough, we've contributed these innovations right back to the community into open source. At Google Cloud, we're firm believers in an open cloud future where vendor lock in is a practice of the past and customers' data belong to them. Because at the end of the day, cloud is about connecting people to the information they need in order to be successful.

Here's to your future.

Brian Stevens
VP Cloud Platforms
Google Cloud

HOW TO PLAN FOR A MULTI-CLOUD WORLD

An open-source strategy and consistent governance will help companies use multi-clouds to compete in the digital world.

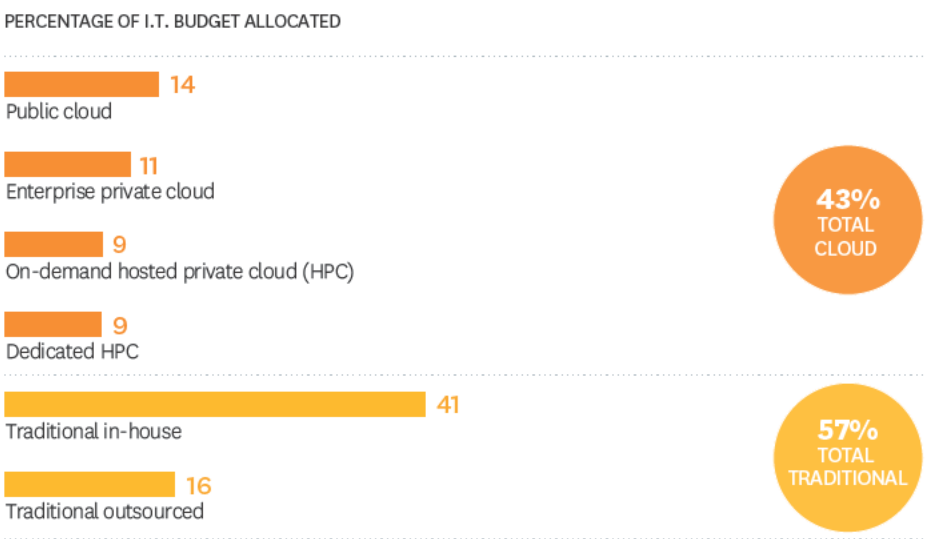
Cloud platforms are rewriting the way that companies work, serving as a vital foundation for digital transformation. By improving business speed and flexibility, cloud helps organizations go to market faster with better products and services. "Cloud's value lies in how fast you can serve customers and deliver new functionality to them," says Jeff Kaplan, managing director at THINKstrategies, Inc.

With Forrester predicting that the public cloud market will hit $191 billion by 2020, the cloud is in hypergrowth mode. Indeed, many large organizations already depend on mixed networks composed of multiple cloud service providers, third-party cloud platform vendors, and on-premises systems. As IDC sees it, cloud purchases across several categories will command 43 percent of the total IT budget by 2018. figure 1

FIGURE 1

I.T. MARKET IN TWO YEARS: GROWTH IN ALL TYPES OF CLOUD

On average, 43 percent of total annual IT budgets will be allocated to cloud-based procurement/management models by 2018.



SOURCE IDC CLOUDVIEW 2016, FEBRUARY 22, 2016

The increase in cloud service consumption manifests itself in several usage models. Today, many organizations are implementing hybrid cloud, which uses a mix of private clouds, public clouds, and legacy data centers. For example, a majority (56 percent) of large enterprises currently use two or three application development platforms in cloud. figure 2

"The biggest trend we're seeing is the combination of cloud and non-cloud IT assets," says Cassandra Moshian, an analyst at TBRI Research. "Enterprises do not necessarily want their existing investments to fall away because of cloud. Rather, they want to utilize cloud to augment and improve what they already have."

According to RightScale's 2016 State of the Cloud report, a commanding 82 percent of enterprises have a hybrid-cloud strategy, running applications in an average of 1.5 public clouds and 1.7 private clouds. This model reflects today's rapidly changing business world, which has one foot in the digital future, while still depending on legacy systems.

Ultimately, however, hybrid cloud helps companies build a foundation for the next generation of cloud consumption, known as multi-cloud usage. Already in use at more bleeding-edge companies, the multi-cloud model allows companies to consume multiple cloud services from multiple vendors in response to targeted business needs. By mixing and matching specific features from different vendors, companies can swiftly respond to customers, partners, suppliers, and employees as their needs change—and significantly scale back, if not ultimately replace, their on-premises systems.

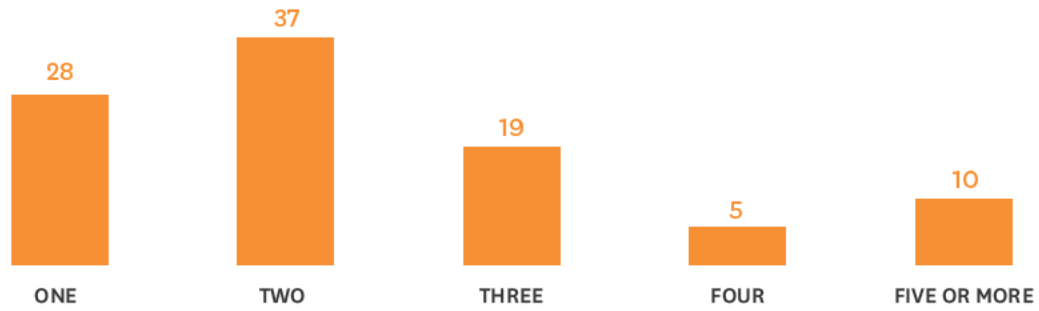
Multi-cloud environments are growing as organizations see the value of expanding their cloud platform portfolio as the fastest way to better serve customers, partners, suppliers, and employees. Price flexibility is perceived as another major benefit. "Companies are realizing that once they get comfortable with one cloud, it often makes sense to look at the specific capabilities of others in certain circumstances," says Joey Jablonski, vice president and principal architect at cloud consultancy Cloud Technology Partners.

FIGURE 2

CLOUD APPLICATION DEVELOPMENT PLATFORMS UTILIZED

Adoption of multiple cloud platforms becoming more common at many enterprise-size companies.

PERCENTAGE INDICATING THE NUMBER OF APPLICATION PLATFORMS IN USE



SOURCE "CLOUD DEVELOPER & PLATFORM RESEARCH," TBRI RESEARCH, 2016

Multi-cloud environments are growing as organizations see the value of expanding their cloud platform portfolio as the fastest way to better serve customers, partners, suppliers, and employees.

For example, one of Jablonski's clients—a large consumer electronics company—recently moved its supply chain and analytics applications from one cloud platform to another to leverage specific data visualization features offered by the second vendor. Adding cloud platforms not only helps organizations avoid vendor lock-in with cloud providers but also provides valuable redundancy.

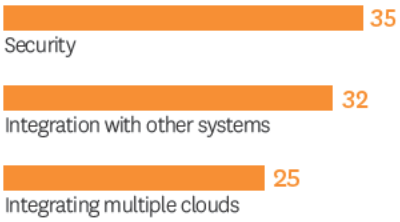
MULTI-CLOUD PLATFORM MANAGEMENT

While spreading applications and workloads across multiple cloud platforms offers undoubted benefits, the practice can also give rise to new integration and management challenges. For example, Kaplan says it's easy to underestimate the work needed to provide a consistent user interface for developers and business users alike across multiple cloud and on-premises platforms. Moreover, ungoverned expansion onto multiple cloud services and platforms can result in integration and management headaches that unnecessarily drive up costs. "The digitization of the world is well underway, and companies always grapple with change when they face such large transitions," as Kaplan puts it.

According to a recent Harvard Business Review Analytic Services study of business managers in large organizations, integration issues involving multiple systems and clouds are perceived to be among the top barriers to employing more cloud platforms today. figure 3 In many cases, companies run into integration problems as they try to migrate workloads from one cloud to another, just as can happen when migrating on-premises applications between platforms. This is especially true when systems use proprietary standards not designed for multi-vendor integration in the first place.

FIGURE 3

TOP BARRIERS PREVENTING ORGANIZATIONS FROM EMPLOYING MORE CLOUDS



SOURCE "HYBRID IT TAKES CENTER STAGE," HARVARD BUSINESS REVIEW ANALYTIC SERVICES, NOVEMBER 2015, N=310

> More and more services are taking an open-source approach, which reduces the time and effort it takes for customers to reconfigure data to match the service provider.
>
> **JEFF KAPLAN, MANAGING DIRECTOR, THINKSTRATEGIES, INC.**

While major cloud providers offer capable management platforms, some focus primarily on their own applications. This forces IT to deploy and maintain multiple management interfaces across the environment. "If companies cannot connect and consolidate management tasks, it can add another layer of complexity," says Kaplan of THINKstrategies.

Data security and regulatory compliance requirements also highlight the need for a cohesive multi-cloud management strategy for data residing on multiple platforms using different security standards. According to Carl Brooks, an analyst at 451 Research, more than 80 percent of the companies he works with cite compliance across multiple systems and platforms as a primary concern when evaluating hybrid- and multi-cloud models. That's when "the conversation gets much more complicated than just better, faster, and cheaper," he says.

BEST PRACTICES FOR BUSINESS IN A MULTI-CLOUD WORLD

As companies move to hybrid- and multi-cloud computing, many leading enterprises are curbing unmanaged cloud expansion by choosing to work with a limited set of platforms that best support specific business goals. "A multi-cloud environment is not only an IT alternative, it's becoming a business imperative—and corporate leaders are getting more involved in such strategies," Kaplan says. To effectively support digital growth and transformation, those platforms must be able to work seamlessly with other platforms, making an open-source approach increasingly important.

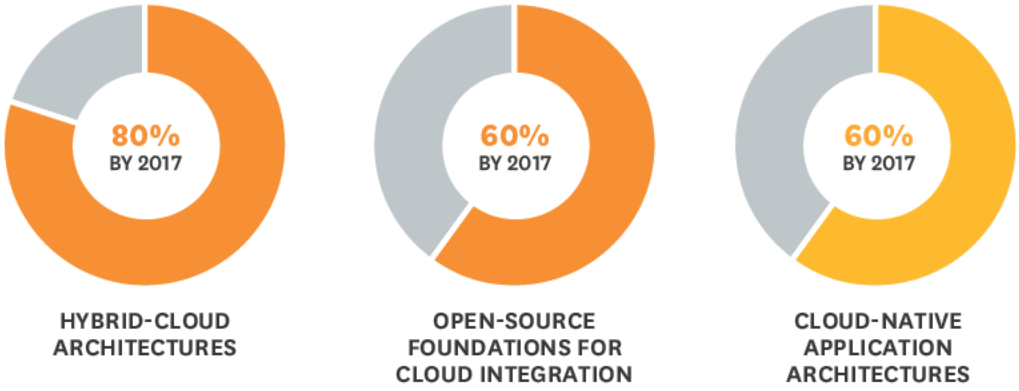
The open-source community is largely driving cloud computing standards in response to strong business demand for cloud adoption. According to a 2016 cloud platforms and standards report from Forrester, 59 percent of decision makers from companies in North America and Europe that consider cloud a high priority said they plan to increase their use of open-source technology over the next 12 months. Indeed, the report notes that OpenStack, the de facto standard for private clouds, is used by 50 percent of Fortune 100 companies.

"More and more services are taking an open-source approach, which reduces the time and effort it takes for customers to reconfigure data to match the service provider," Kaplan says. Doing so also helps companies reconcile the different ways data is stored and organized across service tiers within one cloud platform.

"With multi -cloud, it's even more critical to use open source," adds Jablonski. "It allows companies to pick up apps and move them without having to refactor the apps." Indeed, IDC predicts that companies will increasingly turn to open source as a foundational element for cloud integration in 2017. figure 4

FIGURE 4

INCREASED ADOPTION PREDICTED FOR OPEN SOURCE, HYBRID CLOUD



SOURCE "WORLDWIDE CLOUD 2016, TOP CLOUD TRENDS," IDC FUTURESCAPE

The ability to enforce governance policies across multiple platforms is also key. In addition to certifying each cloud vendor's individual ability to comply with pertinent regulatory environments, enterprises must also find a way to centralize and apply corporate governance, security, and compliance policies across today's hybrid environments. "Policies and controls should not waver across different cloud platforms," says Jablonski. "Security should be uniform from a corporate and governance perspective, including processes for how to respond to incidents and events."

While some leaders may worry that strict governance policies will limit agility and speed, Jablonski considers them the foundation of strategic success. More and more experienced organizations acknowledge the need for centralized governance policies. The IDC 2016 State of the Cloud report found 38 percent of respondents have now established governance policies for cloud, up from 30 percent in 2015.

"I have a client who thinks governance is a bad word," says Jablonksi. "That's unfortunate, because governance is what ensures consistency across the organization." Increasingly, more experienced organizations are implementing a centralized management layer and automated tools to help bake policy compliance into their systems whenever possible.

Finally, leading organizations frequently use third-party support as part of their multi-cloud strategies. For example, many seek help not only selecting cloud providers, but also making sure they get their money's worth. "Navigating service level agreements and the policies and procedures of each provider is just as important as understanding the architecture of those services," Kaplan says. "That's where lots of companies need help."

According to Brooks, nearly 90 percent of the companies he speaks with today use a partner to help manage multiple cloud vendors. "They help companies know where responsibility for things like maintenance and monitoring changes is across the environment," says Brooks. "And that's one of the most important things you need to understand."

Companies should brace for challenges that will need to be met as they transition from in-house systems to hybrid-cloud, multi-cloud, and public-cloud environments.

SUMMARY AND CONCLUSION

As organizations move further into the digital economy, they will increasingly implement new business processes that rely on flexible and secure interaction among multiple cloud environments as well as legacy systems. While cloud computing and use of cloud applications will continue to grow exponentially, companies should brace for challenges that will need to be met as they transition from in-house systems to hybrid-cloud, multi-cloud, and public-cloud environments. Chief among these are dealing with the business and technical issues of security, system integration, compliance, and complexity.

Fortunately, leading organizations are far enough into their cloud transitions to provide advice to later adopters. Among best practices they recommend:

- Leverage open source for interoperability
- Standardize governance across platforms and tools
- Centralize management
- Rely on third-party support

By evaluating mechanisms such as open source and cloud management in conjunction with new approaches within IT, organizations can build a cohesive strategy for living in a multi-cloud world.

hbr.org/hbr-analytic-services

Harvard Business Review

EXHIBIT M

Attachment J-8

Joint Enterprise Defense Infrastructure (JEDI) Cloud
JEDI Cloud Definitions
Updated 23 July 2018

1 Purpose

While other definitions of these terms and acronyms may exist, these are the specific definitions that apply to the JEDI Cloud requirement unless a particular JEDI Cloud document defines the term otherwise, in which case the other document is controlling.

2 Definitions

1. **Account** - See JEDI Cloud Cyber Security Plan.

2. **Addressing** - See JEDI Cloud Cyber Security Plan.

3. **Administrative Access** - See JEDI Cloud Cyber Security Plan.

4. **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.

5. **Allocation** - See JEDI Cloud Cyber Security Plan.

6. **Antifragile** - See JEDI Cloud Cyber Security Plan.

7. **Application Programming Interface** (**API)** - A system that supports modern protocols such as HTTPS for the purpose of machine-to-machine data transmission, both for reading and writing data.

8. **Application** - See JEDI Cloud Cyber Security Plan.

9. **Application Server** - Physical infrastructure where the end user loads a commodity operating system and at least two application runtimes into a virtualized environment hosted on the physical servers (for example, a network router would not satisfy this definition of application server).

10. **AT-AT** - The DoD's provisioning tool, known as the Account Tracking and Automation Tool (AT-AT), will manage user identity, access control, billing configuration, and security and configuration policy compliance for the purposes of accessing the JEDI

Cloud. All automation and integration will be centrally managed by the CCPO.

11. **Availability Zones / Regions** - Availability zones have independent power and network backbone. A “region” of a cloud service provider would encompass multiple availability zones such that systems and data in a region with a failed availability zone could seamlessly transfer to another zone and continue operation.

12. **Bring Your Own License (BYOL)** - The ability of a JEDI Cloud user to deploy software or platform offerings from the online marketplace into JEDI Cloud without additional licensing cost for that software or platform offering because the JEDI Cloud user already possesses a valid license from a separate contracting action.

13. **Classified infrastructure** - See JEDI Cloud Cyber Security Plan.

14. **Classified media** - Any device which is capable of storing data used in classified infrastructure.

15. **Closed-loop system** - System that is able to operate with no external connectivity.

16. **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 document, cloud refers to physical computing and storage resources pooled to provide virtual computing, storage, or higher-level services.

17. **Cloud Boundary** - Physical boundary between the JEDI Cloud and any external systems, or networks.

18. **Commercial cloud** - Means that a commercial cloud service provider is maintaining, operating, and managing the computing, networking, and storage resources that are being made available to customers. Depending on the contract, the commercial cloud service provider may be performing in commercial facilities or on premises.

19. **Commercial Cloud Offering (CCO)** - Defined as the IaaS and PaaS offerings that are publicly-available and currently sold in the commercial marketplace, but excluding any Software as a Service (SaaS) offerings.

20. **Commercial Parity** - Equivalency of the services and capabilities offered between the JEDI Cloud and the contractor’s publicly-available commercial cloud in the continental

United States.

21. **Cryptographic certainty** - See JEDI Cloud Cyber Security Plan.

22. **CSP** - Cloud Service Provider or Cyber Security Plan depending on context.

23. **Data center** - See JEDI Cloud Cyber Security Plan.

24. **Elastic** - Capabilities that can be provisioned and released to scale outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be provisioned in any quantity at any time.

25. **Erase** - Apply logical techniques to sanitize data in all addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). The term Clear in NIST SP 800-88 Revision 1 is similarly defined.

26. **Failover** - See JEDI Cloud Cyber Security Plan.

27. **Federated identity** - an assured process that allows for the conveyance of authentication and subscriber attribute information across networked systems, in this case between the CCO vendor's identity management system and DoD systems.

28. **Hypervisor** - a collection of software modules that provides virtualization of hardware resources (such as CPU/GPU, Memory, Network and Storage) on a single physical host.

29. **Impact Level 5 (IL5)** - See JEDI Cloud Cyber Security Plan.

30. **Impact Level 6 (IL6)** - See JEDI Cloud Cyber Security Plan.

31. **Infrastructure** - See JEDI Cloud Cyber Security Plan.

32. **Infrastructure as a Service (IaaS)** - The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able 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).

33. **Investigation** - See JEDI Cloud Cyber Security Plan.

34. **IV&V Testing** - Independent Verification & Validation. An independent system assessment that analyzes and test the target system to 1) ensure that it performs its intended functions correctly, 2) ensure that it performs no unintended functions, and 3) measure its quality and reliability.

35. **Logical Separation** - See JEDI Cloud Cyber Security Plan.

36. **Machine Learning (ML)** - a statistical process that starts with a body of data and tries to derive a rule or procedure that explains the data or can predict future data rather than programming specific rules to explain data or predict future data.

37. **Migration** - the act of moving an application from one infrastructure or platform to another infrastructure or platform.

38. **Mitigation** - See JEDI Cloud Cyber Security Plan.

39. **Meet Me Point** (**MMP)** - A connection to or from the DoDIN or other DoD networks from the cloud service provider.

40. **Nearline storage** - Storage not immediately available, but can be brought online quickly without human intervention.

41. **Network** - See JEDI Cloud Cyber Security Plan.

42. **Offline Storage** - Data not immediately available, requiring some human or scheduled intervention to become online. Also known as Cold Storage.

43. **Online storage** - Storage that is immediately accessible to applications without human intervention.

44. **Platform as a Service (PaaS)** - The capability provided through software, on top of an IaaS solution, that allows the consumer to replicate, scale, host, and secure consumer-created or acquired applications on the cloud infrastructure. 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 application hosting environment configurations.

45. **Points of Presence** - A demarcation point or interface point between communicating entities.

46. **Provisioning** - In the context of the JEDI Cloud contract, “provisioning” is the act of creating something in the cloud environment (*e.g.*, accounts, compute instances, users, storage mechanisms) in either a manual or automated fashion.

47. **Purge** - Apply physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques.

48. **Resource pooling** - The provider’s computing resources are pooled 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 location of the provided resources but may be able to specify location at a higher level of abstraction (*e.g.*, country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

49. **Robust Infrastructure** - Assured infrastructure that is responsive, resilient, redundant, and reliable.

50. **Role** - A job function, with associated privileges, to which people or other system entities may be assigned in a system.

51. **Ruggedized** - System specifically designed to meet or exceed MIL-STD-810G standards to ensure reliable operations in harsh usage conditions. Whether the system needs to be tested and certified as meeting the standard is at the discretion of the Government.

52. **Self-service** - The ability of an end-user to access data and perform actions without any human interaction or third party approval.

53. **Server** - See JEDI Cloud Cyber Security Plan.

54. **Software as a Service (SaaS)** - The capability provided to the consumer is to use the provider’s 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 email). 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.

55. **Tactical Edge** - Environments covering the full range of military operations, including, but not limited to forces deployed in support of a Geographic Combatant Commander or applicable training exercises, on various platforms (*e.g.*, dismounted infantry patrol, forward operating base, and aircraft carrier) and with the ability to operate in austere and connectivity-deprived environments.

56. **Tactical Edge Device** - Durable and portable computing and storage capability able to operate in the tactical edge.

57. **Testing** - See JEDI Cloud Cyber Security Plan.

58. **Traffic** - See JEDI Cloud Cyber Security Plan.

59. **Unclassified infrastructure** - See JEDI Cloud Cyber Security Plan.

60. **User** - Provisioned identity able to manage infrastructure.

61. **U.S. Person** - The term "United States person" means any United States citizen, any alien lawfully admitted for permanent residence in the United States, and any corporation, partnership, or other organization organized under the laws of the United States that is not under the control of a foreign government.

62. **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.

63. **Virtual Machine** (**VM)** - Software that emulates the physical hardware of a computer.

64. **Vulnerability** - See JEDI Cloud Cyber Security Plan.