Attachment L-1

Joint Enterprise Defense Infrastructure (JEDI) Cloud
Statement of Objectives (SOO)
As of 22 August 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 the conclusion of the post award kickoff event 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 the conclusion of the post award kickoff event. 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 the conclusion of the post award kickoff event.

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 workspace, 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 workspaces or all workspaces 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 ultimately available on all continents (except Antarctica) through two or more connections providing a total bandwidth capacity of at least 40 Gigabits per second.

3.2.2.1 Compliant points of presence must be active and available for use on all continents except Africa and Antarctica at the time of proposal submission.

3.2.2.2 One or more compliant points of presence must be located in Africa, active, and available for use within 30 days of the conclusion of the post award kickoff event.

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 a workspace to include workspace 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 workspace within the cloud environment.

3.8 Provide cloud-service usage and billing reports for all workspaces under the JEDI Cloud contract and by specified workspace(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 workspaces and all workspaces 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 workspace level and for all workspaces 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 workspaces and for all workspaces 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 workspace 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 workspace, and under the entire JEDI Cloud contract; and

3.9.1.6 Setting billing and usage thresholds and adding automated notifications to workspace 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 data center locations providing unclassified JEDI Cloud services and no fewer than three physical data center locations providing classified JEDI Cloud services within the Customs Territory of the United States, as defined in FAR 2.101. Each classification level requires its infrastructure to be hosted in 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.

3.15.2.1 Each data center must be capable of automated failover of computing, network and storage services to one another within a classification level.

3.15.2.2 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 (both Secret and Top Secret) 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 workspace. 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 workspaces 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 price-free, excluding the cost of IaaS resources, or where the DoD already possesses a license using the bring your own license (BYOL) approach. At least 90% of all price-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 workspace.

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 Include the capability to control the 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).

3.19.12 The Government will not order any tactical edge devices (including both static, modular, rapidly deployable data centers and portable devices) until the first unit is assessed and authorized within each classification level.

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 workspaces 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	Sent within 10	99%	Vendor log

	notifications for budgeting and usage based thresholds	minutes of crossing threshold		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	Under 1 second, excluding query processing time	99%	Database and network log analysis

	zones			
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	Within 5 minutes, excluding time spent waiting for actions being taken by 3rd parties and the time required for any required infrastructure to start up.	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

505
506 * All performance metrics apply to tactical edge capabilities unless explicitly stated otherwise.
507 For unclassified and classified tactical edge devices that are deployed, accepting any
508 modifications to the services and offerings are at the discretion of the JEDI Cloud user. If a JEDI
509 Cloud user does not accept a modification, the Offeror is not responsible for meeting
510 Performance Metrics that are directly affected by the JEDI Cloud user's decision.
511
512 **Constraints**
513
514 Any constraints are provided elsewhere in the SOO or listed in the Cyber Security Plan.
515
516 **Deliverables**
517

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	Electronic copy in Offeror's preferred format	CCPO

		thereafter		
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.