

[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



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 warfighter 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*



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



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:



- 
- 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 advises, "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 military Services, 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.

DoD FY 2019-2023 Future Years Defense Program Cloud Computing

(dollars in thousands)

<u>Cloud Type</u>	<u>FY 2019</u>	<u>FY 2020</u>	<u>FY 2021</u>	<u>FY 2022</u>	<u>FY 2023</u>	<u>FYDP</u>
<i>Commercial Cloud</i>	106,816	122,331	93,829	100,997	101,419	525,392
<i>Other Cloud</i>	286,370	377,926	145,951	147,588	142,604	1,100,439
<i>Total FYDP</i>	393,186	500,257	239,780	248,585	244,023	1,625,831

Note: Includes \$160M in FY 2019 and \$260M 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

