Senate Finance Questions

Body Text

"Cloud computing and storage provide the necessary foundation to adopt modern software practices and emerging technologies, such as artificial Intelligence (AI)." This implies that the current cloud system is not adequate as a foundation. Why is that? How does Jedi create a superior foundation? Can the current systems no be modernized?

There are fundamental differences in the way cloud computing stores and processes data that enable high compute efficiency that cannot be accomplished with older technology. Current systems can either be modernized to run in cloud computing environments or be totally rebuilt, depending on the age and other technical factors. By leveraging commercial cloud computing environments for hosting systems and applications, DoD is able to stay current with new technology, while eliminating up-front investment for traditional hardware infrastructure. Additionally, by leveraging commercial cloud services DoD inherits innovation from one of the most hotly contested areas of industry in which investment in new capability and cyber security far outstrips available Government spending.

Modern software practices require consistency in the underlying infrastructure in order to allow for continuous development, automation, and speed. Emerging technologies, such as machine learning (ML) and artificial intelligence (AI), require an enormous amount of elastic, auto-scalable compute and storage to work. Architecting on-premise, data center solutions to address the needs of modern software practices and emerging technologies is technically challenging, if even possible, and often cost prohibitive.

Cloud solutions currently being used across DoD are uncoordinated and disparate, which creates barriers to optimizing data and applying consistent modern software practices across the Department. JEDI addresses the foundational needs to enable modern software practices and emerging technologies, such as AI, in a more cost effective manner than attempting to undertake the technically complex operation of modernizing data centers.

Questions

1) What internal policies does the Department have in place to ensure that Requests for Procurement [sic] (RFP) and subsequent government contracts are not drafted so that they are tailored to match the specific technical capabilities of a particular company when that company does not qualify for a sole source contract as per Federal Acquisition Regulation (FAR) 6.101 and FAR 3.301? Were these policies adhered to in this case?
    a. What evidence can you share that would provide assurances to this effect?
    b. Is it OSDs position that <u>ALL</u> regulations were followed?

The DoD acquisition process is governed by numerous statutory and policy requirements that ensure competition in contracting. The process includes multiple levels of internal review and oversight including legal review of requirements to ensure procurements are not tailored to a specific vendor.

Appropriate legal review occurred in addition to Department acquisition authorities reviewing the JEDI requirements prior to finalization and release of the RFP on July 26, 2018. DoD maintains, and GAO found in their November 14, 2018 decision, that all regulations were followed in the creation of the JEDI RFP. More than one company satisfied the DoD criteria and are actively competing for the award.

2) Please provide copies of current Department policy and procedures that address potential conflicts of interest in the contracting process. Please include any policies and procedures that address roles and responsibilities in drafting contracts and requests for proposals, and in reviewing those processes for potential conflicts.

As stated in our original response, there are a host of ethics laws and regulations, applicable to all Executive Branch agencies, that are designed to identify and avoid potential conflicts of interest, including the conflicts of interest laws at 18 U.S.C. §§ 207 and 208, the financial disclosure reporting requirements at 5 U.S.C. app. 101, et. seq., and implementing ethics regulations at 5 C.F.R. Chapter XVI, Subchapter B and FAR) at 48 C.F.R. Part 3. In addition to these provisions, DoD has implemented supplemental requirements in the Joint Ethics Regulation, DoD 5500.07R, and the DFARS, 48 C.F.R. Part 203. Individuals who meet the statutory and/or regulatory filing criteria are required to submit financial disclosure reports setting forth their financial interests and affiliations, which are reviewed by supervisors and ethics counsel. These individuals are required to receive ethics training annually.

Under FAR 1.602-2, the contracting officer must ensure that all contractors receive impartial, fair, and equitable treatment. Further, under FAR 3.104-7, the contracting officer must investigate a violation or possible violation of the procurement integrity rules and determine if the reported violation or possible violation has any impact on the pending award.

a. When and how often are these documents reviewed and checked for accuracy?

Individuals who meet the statutory and/or regulatory filing criteria are required to submit financial disclosure reports (*i.e.*, SF 450 and SF 278), upon entering new positions and annually thereafter, setting forth their financial interests and affiliations. Financial disclosure reports are reviewed by supervisors and ethics counsel. Filers are required to

receive ethics training annually. In addition, DoD requires that all Defense Acquisition Workforce personnel receive annual ethics training.

Additionally, individuals participating in a source selection process are required to disclose their financial interests and affiliations and receive procurement integrity training prior to participating in the source selection process.

Employees are responsible for disclosing any potential conflicts, and any falsification of information or failure to file or report required information may result in disciplinary action or criminal prosecution.

The forms and procedures articulated above apply to all Federal agencies and are not unique to DoD.

b. The department ALWAYS adheres to all acquisition and ethics laws? Under current laws, are former employees of 'Company A' now working for DOD allowed to help design a contract that that 'Company A' will likely bid on? When? What if that former employee that is now working for DOD has already accepted a position back with 'Company A'?

As stated in Answer 2 above, there are a host of ethics laws and regulations designed to identify and avoid potential conflicts of interest.

These laws and regulations govern both criminal and civil conflict of interest matters and prohibit parties from participating in matters where they have a real or imputed interest. All DoD employees are required to take annual ethics training, which includes review of potential scenarios to guide employees. Employees are strongly advised to consult with ethics counselors, who are specially trained to apply the ethics rules, whenever a question arises. Ethics advice is tailored to the unique facts and circumstances of the situation.

Failure to adhere to either self-reporting guidelines or ethics counsel guidance are referred to the appropriate investigating authorities.

In addition, there are laws and regulations that address post-employment ethics restrictions of former Government employees. When individuals fail to comply with the laws during or after their DoD employment, they are subject to a range of penalties for failure to do so, including referral to the Department of Justice for criminal prosecution.

Again, the DOD followed <u>ALL</u> of its procedures? What was the reasoning behind the contracting officer's decision? Is this is the same or one of the same contracting officers that worked on the initial formation of the JEDI contract? The phrasing of this sentence implies recognition that something did not meet DOD standards regarding the acquisition contract, but that this did not impact the 'integrity of the acquisition.' What did not meet DOD's standards? How can we stop a reoccurrence? What do you mean that it did not impact the 'integrity of that acquisition?" has this determination been made by any third party contingent in DOD? Regarding the more recent allegations that a DOD employee had already accepted a position with one of the remaining competitor companies: has the DOD verified this information? Did the DOD already know this information when the contracting officer made this determination? Does this in anyway change the determination that was made by the contracting officer? How is this not a conflict of interest? Please provide citation of authorities that allow you to make these determinations.

As stated in Answer 1, the contracting officer's authority and responsibility to investigate conflicts of interest is granted in the FAR. While DoD cannot discuss details of on-going acquisition or litigation activity, the contracting officer conducted an investigation prior to litigation or any facts being made public. GAO upheld the contracting officer's determination in its November 14, 2018 decision. When additional information came to light during the federal court litigation process, DoD unilaterally requested a pause in the litigation work in order to conduct additional investigation.

Based on this new information, the potential conflicts of interest were referred to the appropriate ethics and investigative authorities. Apart from personal conflicts of interest, the contracting officer must determine whether the overall integrity of the acquisition process has been negatively impacted by potential personal conflicts of interest.

DoD followed all applicable laws and regulations, regardless of assertions to the contrary. Oracle exercised its right to protest DoD's actions in JEDI, and the federal judge will issue a decision on the conflicts of interest allegations.

3) Department officials have reportedly described JEDI Cloud as a "pathfinder" intended to provide a model for the Department's future transition of legacy IT systems to the cloud Please describe any related efforts to ensure full and open competition for future Department cloud services contracts.
   What is a "pathfinder?" How does the JEDI contract compare to contracts for other "pathfinders?" How was the determination made that this was going to be a sole source contract? What about this program requires it to be a sole source contract? How does this determination work within DOD's cloud strategy?

   a. Please provide examples of fit for purpose vs. general purpose clouds. Is it DOD's goal to have a SINGLE cloud (we discussed this in our meeting)?

DoD's 2018 Cloud Strategy details both the overall cloud approach and JEDI's role within that strategy. The strategy envisions a multi-cloud, multi-vendor future with JEDI as the focal point for building organizational discipline in the areas most relevant to general purpose cloud computing. The multi-cloud approach is both the intended future state and the current reality for DoD with additional contract vehicles for enterprise fit-for-purpose cloud (as defined by the strategy) efforts totaling more than $8.5B already awarded or currently being acquired through a separate effort. Examples include the currently

awarded milCloud 2.0 contract and the DEOS contract vehicle for SaaS productivity software currently being acquired through a separate effort. Ultimately, DoD intends to leverage JEDI pathfinder to develop the organizational competencies and processes necessary to operate effectively in the general purpose cloud environment (see notes on challenges with the current multi cloud environment in Answer 5). This strategy closely mirrors the approach successfully adopted by the Intelligence Community.

With respect to the questions regarding a sole source determination for JEDI, it is worth re-stating that JEDI is not a sole source acquisition. On the contrary, JEDI is enabling fierce competition among some of the largest and most innovative companies in the industry. The JEDI Cloud acquisition activity is a fair and open competitive source competition in full compliance with all applicable laws.

4) In a May 2018 report to Congress, the Department indicated that the "underlying documentation required by the Federal Acquisition Regulation to support the single award ID/IQ approach is still under development within the Department. " The Department also said that it would not release the final JEDI solicitation until it executed the underlying justification documents. Please provide the Department's justification supporting the use of a single award ID/IQ approach for the JEDI contract.
    a. Please PROVIDE a copy of this document and any supporting documents that were utilized in the decision making process to form this document.

A copy of the document supporting the single award ID/IQ approach is attached.

5) In September 2018, the OMB published their CLOUD SMART Strategy Proposal. How does the JEDI program and procurement process align with the Federal government-wide strategy outlined in the aforementioned document?
    a. Is this strategy a sound one? How many large private companies utilize similar models? How is it advantageous? How is what we have now substandard? Is this worth the cost? Sell the program. Please explain the “grocery store” model here (or wherever it is the most appropriate).

DoD’s current investments in cloud computing, which span numerous contracts with nearly every major cloud provider, are fragmented. The lack of enterprise coordination and guidance has led to Departmental inefficiencies and has hindered the Department in IT modernization efforts. It has led to disparate efforts with siloed teams, disjointed implementations with limited capability, siloed data, and inefficient acquisitions that cannot take advantage of economies of scale.

Anticipated improvements in time-to-capability for software, software resilience, and cyber security have not been broadly realized across the Department. In addition, the current

environment has not provided the warfighter access to readily available compute resources globally across classification levels and in the tactical environment as required by JEDI. JEDI is designed to improve the current state by shifting the focus from cloud acquisition to cloud maturity in DoD's business processes related to cyber security, application development, and workforce development. This approach mirrors many of the recommendations in the Federal Strategy as highlighted in our original response and follows the path adopted by the Intelligence Community.

Additional Questions

1) How long will it take to migrate all of the proposed information onto the new JEDI server, if the server was used at its max capacity?

There is no established consumption target in terms of systems, data, or dollars for the JEDI program. The $10B contract ceiling establishes a maximum value for the contract itself, but decisions regarding the movement of individual applications and datasets rest with the DoD components. DoD anticipates that data and application migration will continue throughout the program lifecycle.

2) With all of the controversy surrounding this contract what are the reasons for not pulling the RFI and resubmitting it? Especially when you consider that historically when the DOD has done this in the past the price to the taxpayer has been significantly less.

DoD acquisitions must be driven by the needs of the warfighter. The Department's requirements for cloud computing were extensively and thoroughly vetted over a long period of time. The requirements, which have not changed substantially, drove the acquisition approach. DoD remains confident that fierce competition within the framework of the existing acquisition will drive favorable pricing.

3) On September 13, 2017, you issued a Memorandum entitled "Accelerating Enterprise Cloud Adoption." As part of that memorandum, you established the Cloud Executive Steering Group (CESG) and appointed one CESG member, the Director of the Defense Digital Services (DDS), to lead Phase One of DoD cloud adoption, which would use a "tailored acquisition process to acquire a modern enterprise cloud services solution that can support unclassified, secret and top secret information."[1] I understand until very recently, the Director of DDS was Mr. Chris Lynch.
    a. Can you point to anywhere in the 13 September memorandum where you reference a multi-cloud, multi-vendor environment?
    b. Can you tell me what you meant by a "tailored acquisition process," which is not a term that is familiar to me from the FAR? Is that somehow different from the full and open competition we would expect for a contract of this magnitude?

[1] https://www.nextgov.com/media/gbc/docs/pdfs_edit/090518cloud2ng.pdf

c. Can you tell me how the DDS is set up to manage a procurement of this magnitude as opposed to normal Department procurement channels?

d. Can you provide me with Mr. Lynch’s background prior to heading DDS, which would qualify him to lead the largest IT procurement in history? Did he have enterprise modernization expertise? Had he led a major cloud migration? Had he ever managed a major IT procurement? Does he have any formal technical training? Please include a copy of his CV with your response.[2]

The September 2017 memorandum establishing the accelerating to cloud initiative specifically identifies a multi-cloud strategy where it states: “The Department will establish a Cloud Executive Steering Group (CESG) to devise and oversee the execution of a strategy to accelerate the adoption of cloud architectures and cloud services, focusing on commercial solutions.” (emphasis added) As the CESG, and then ultimately DoD CIO, guided the evolution of the acceleration to cloud initiative, the high level initiative matured into the more specific 2018 DoD Cloud Strategy, which explains how JEDI is one component of a multi-cloud ecosystem. The JEDI acquisition is consistent with that strategy.

All acquisitions within DoD are tailored consistent with the guidelines set forth in the FAR, DFARS, and DoD internal policies to best meet the needs of individual programs. The contracting officer has the authority to make these tailoring decisions in consultation with the acquisition governance processes within the Department. This term has no specific meaning related to full and open competition. JEDI was fully and openly competed with 4 of the 5 major (non-Chinese) cloud providers as identified by Gartner choosing to compete.

While the Defense Digital Service did incubate the JEDI concept and provided technical and engineering support for the development of the JEDI Cloud RFP after the Accelerating Enterprise Cloud Adoption memo (13 September 2017 memo); responsibility for JEDI Cloud was transferred to the DoD Chief Management Officer in January 2018. In June 2018 responsibility for JEDI Cloud was formerly transferred to DoD CIO with the arrival of Dana Deasy. This transfer of responsibility took place prior to the release of the JEDI RFP.

4) Can you reference any slides or documents from JEDI Industry Day that reference JEDI as a “pathfinder” or that discuss multi-cloud or multi-vendor environments? When was this term first used? When was it first provided a definition?

JEDI’s role as a pathfinder was first described publicly in summer, 2018 and was finalized in the DoD Cloud Strategy in December 2018. The strategy itself was influenced by input from many sources including comments received from industry throughout the JEDI acquisition process. The term ‘pathfinder’ is commonly used in defense programs to denote pilot, proof-of-concept, or other learning-oriented programs.

[2] https://www.linkedin.com/in/lynchseattle/

5) On November 6, 2017 DoD issued document summarizing the newly created JEDI program highlighting the use of a “single Cloud Service Provider (CSP) to deliver services for cloud computing infrastructure and platform services.”[3] Can you point to any reference in that document that refers to a multi-vendor, multi-cloud solution or that refers to JEDI as a pathfinder?

On February 15, 2018, DoD publicized a JEDI FAQ on its website and explained that the November 6, 2017 document was actually a “draft document used to spark discussion and debate” within DoD, and that “the [Cloud Executive Steering Group] is still in the analysis and fact finding phase of this process to determine how many contracts will best meet DoD’s needs.” Additionally, the formation of the JEDI program predates the 2018 Cloud Strategy that formally documented JEDI’s role within the larger cloud ecosystem.

6) Can you confirm that only four vendors responded to your JEDI RFP, including Amazon, IBM, Microsoft and Oracle and that two of those vendors IBM and Oracle were eliminated for failing to meet JEDI’s “gate criteria”? Can you confirm that Google decided not to submit a bid and according to a Google spokesperson said, “had the JEDI contract been open to multiple vendors, we would have submitted a compelling solution …?”[4] If IBM, Oracle and Google do not qualify to participate in JEDI, can you explain how you intend to implement a multi-cloud, multi-vendor environment with three clearly capable U.S. cloud infrastructure and platform vendors excluded?

There are only a handful of non-Chinese companies in the world that can provide general purpose cloud capabilities on the scale required for the Department of Defense. IBM, Oracle, Microsoft, and Amazon bid on JEDI. These companies represent four of the five hyper scale Infrastructure-as-a-Service (IaaS) companies as identified by Gartner. DoD cannot comment on a vendor’s decision-making process related to participation in an acquisition. As discussed throughout the 2018 Cloud Strategy there are many opportunities for multi-clouds and multiple vendors for IaaS, PaaS, and software.

7) Since JEDI is now set to be awarded by July 19, 2019, do you believe that down-selecting to two vendors is enough to ensure price competition for the U.S. taxpayer? Why wouldn’t keeping multiple vendors in the competition make more sense to ensure the DoD receives the best price? Is it OSDs position that only two companies are capable and willing to participate in this program?

[3] https://www.nextgov.com/media/gbc/docs/pdfs_edit/121217fk1ng.pdf

[4] https://www.marketwatch.com/story/the-jedi-war-amazon-oracle-and-ibm-battle-in-mysterious-world-of-militarycontracts-2019-01-07

DoD’s position is that the Department carefully collected and vetted requirements, designed and formally approved a competitive acquisition strategy, and executed a competition in accordance with the applicable laws, regulations, policies, as well as the stated RFP criteria. JEDI has tremendous price competition among the cloud providers who submitted proposals. The pricing competition is going to come down to vendors who can provide the full scale of services at the best value. To ensure DoD continues to benefit from global marketplace pressures and maintain best-in-class pricing, the JEDI contract tethers its prices to the vendor’s commercial prices.

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

The Honorable Ellen Lord
Under Secretary of Defense
for Acquisition and Sustainment

JUL 19 2018

Date

Department of Defense

DoD Cloud Strategy

December 2018

FOREWORD

The Department of Defense (DoD) has entered the modern age of warfighting where the battlefield exists as much in the digital world as it does in the physical. Data and our ability to process data at the ready are differentiators to ensure mission success. Cloud is a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining our military's technological advantage.

The DoD Cloud Strategy reasserts our commitment to cloud and the need to view cloud initiatives from an enterprise perspective for more effective adoption. It recognizes our experience over the past five years and identifies seven strategic objectives along with guiding principles to set a path forward. It emphasizes mission and tactical edge needs along with the requirement to prepare for artificial intelligence while accounting for protection and efficiencies.

The strategy drives implementation toward the enterprise cloud environment, an ecosystem composed of a General Purpose and Fit For Purpose clouds. It focuses implementation activities on two fundamental types of work: first is the stand up of cloud platforms ready to receive data and applications, and second is the ongoing work to migrate existing applications and to develop new applications in the cloud.

This effort is a Department priority. As we execute this strategy, we will continue to seek the active participation and commitment of all DoD Components to realize the benefits of cloud as we operate on the 21st century battlefield.

Table of Contents

1 Strategic Environment

"If we fail to adapt ... at the speed of relevance, then our military forces ... will lose the very technical and tactical advantages we've enjoyed since World War II."
- Secretary of Defense James N. Mattis

Information is vital to United States (U.S.) national security and our ability to understand emerging threats, project power globally, conduct operations, support diplomatic efforts, and enable global economic viability. The Department of Defense (DoD) has multiple disjointed and stove-piped information systems distributed across modern and legacy infrastructure around the globe leading to a litany of problems that impact warfighters', decision makers', and DoD staff's ability to organize, analyze, secure, scale, and ultimately, capitalize on critical information to make timely, data-driven decisions. Today, the Department is largely constrained by physical resources, manpower limitations, organic skillsets and, oftentimes, laborious contracting processes to procure or grow storage and computing capabilities. In addition, the cyberspace domain continues to be an increasingly contested environment. In order for the U.S. to keep its strategic advantage, warfighters and the force that support them need to be provided with the proper capabilities and technologies to succeed.

To this end, commercial industry has made significant strides in addressing these challenges that the Department can leverage. Commercial cloud computing is a subscription-based service that provides network-based storage and compute resources. It allows users to store and access data and programs over the Internet rather than on a local computer hard drive. It also allows users to access information from anywhere at any time, effectively removing the need for the user to be in the same physical location as the hardware that stores the data. The Department must take full advantage of this technology enabler.

1.1 Inadequate Efficiency and Security in Information Technology

The physical information technology (IT) infrastructure deployed across the Department was purchased with a "maximum use" case in mind. In other words, the hardware can support the greatest possible expected demand, regardless of how infrequently that may happen, if at all. This causes much of the physical IT infrastructure purchased to be idle the majority of the time. Commercial cloud infrastructure works differently. It can scale dynamically to support resource demands with the benefit of only paying for the actual use. During most times, systems can be scaled down to support the minimal traffic that is the norm.

By owning and operating the physical hardware associated with on-premises data centers, the Department can incur unnecessary security risks and consume resources that could otherwise be realigned to support warfighters and the workforce in other mission areas. A combination of overly strict policies and procurement procedures make it difficult for DoD to ensure that both hardware and software are updated appropriately. The cost spent on physical hardware has a negative impact on diverting vital resources away from the warfighter and workforce as well as security impacts with a direct burden of responsibility for security updates of both hardware and software on DoD. The Department has historically been challenged to keep up with cyber threats to its IT infrastructure.

1.2 Disparate Cloud Efforts and Disjointed Implementation

DoD has not had clear guidance on cloud computing, adoption, and migration to provide unifying guidance or a coherent plan. This has made it difficult for the Department to embrace modern IT capabilities, to benefit from the efficiency and capacity offered by commercial cloud services, and to continue to evolve with technology at the speed of relevance.

The lack of guidance has led to Departmental inefficiencies and has hindered the Department in IT modernization efforts. It has led to disparate efforts with siloed teams, disjointed implementations with limited capability, siloed data, and inefficient acquisitions that cannot take advantage of economies of scale.

1.3 Lack of Cloud Fitness

DoD has stood up a number of clouds that have not been architected or designed for enterprise use. It is imperative that DoD has a cloud strategy to ensure that legacy applications are not moved to cloud without properly rearchitecting them to make use of the data, security, resiliency, and application advantages that cloud provides. Additionally, DoD should independently test and assess cloud network security to verify security compliance and incident response, and review all contractor and third-party testing results to ensure that performance and security monitoring are sufficient. Systems that are not "cloud ready" will most likely use excessive amounts of cloud infrastructure resources, meaning they will not be any more efficient and will almost certainly cost more to operate. This is why system rationalization is critical, but, without proper guidance, many program offices may not do this properly or skip it entirely.

There is currently no enterprise-wide guidance on how to rationalize a system nor for assessing a system's cloud readiness. This gap has further led to the siloed data behavior mentioned earlier and restricted the ability of the Department to share information. This enterprise-wide guidance is imperative to the success of any cloud strategy – enterprise or otherwise.

As DoD has continued to stand up independent clouds, we continue to dilute our already constrained cloud expertise. This enterprise cloud strategy provides the constructs for optimizing our use of cloud talent. To date, the DoD oftentimes relies on outside contracting firms to perform these assessments, never building the organic corporate knowledge to carry us into the future. Decisions are being made at high levels without in-house technical expertise as advisors. The Department must invest in its own future by building technical knowledge within.

1.4 Readiness for Artificial Intelligence (AI)

As DoD embarks to stand up a Joint Artificial Intelligence Center (JAIC), it will require an enterprise cloud infrastructure capability. An enterprise cloud will provide the common data and infrastructure platforms that will enable AI to meet the full promise of warfighter advantage.

DoD has created this DoD Cloud Strategy to align with the larger DoD cyber strategy, strengthening the security and resilience of the networks and systems that contribute to the Department's military advantage.

2 Strategic Objectives

DoD will continue to rely on its ability to process and disseminate information for military operations, intelligence collection, and related activities. To ensure this, the Department must address the unique mission requirements through a multi-cloud, multi-vendor strategy that incorporates a General Purpose cloud and Fit For Purpose clouds (reference Appendix A). To this end, this strategy will design objectives around solving these strategic challenges:

- Enable Exponential Growth
- Scale for the Episodic Nature of the DoD Mission
- Proactively Address Cyber Challenges
- Enable AI and Data Transparency
- Extend Tactical Support for the Warfighter at the Edge
- Take Advantage of Resiliency in the Cloud
- Drive IT Reform at DoD

2.1 Enable Exponential Growth

The pace of data growth is accelerating; in the last two years, the world produced 90% of all existing data. This is a trend that has been going on for a decade, with no end in sight; however, the Department's ability to access all of that data when and where it is needed has not evolved at the same pace. Modern computing capabilities can access, retrieve, manipulate, merge, analyze, and visualize data at machine speeds, providing substantial decision making advantages on the battlefield. To adapt to the continuously growing data environment, 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.

DoD relies on critical intelligence to make vital national security decisions. The quantity and quality of intelligence information has been the tipping point in numerous conflicts. As the quantity of raw information production increases, so does the struggle to organize, analyze, and distribute that information to make critical decisions.

DoD must continue to maintain its strategic advantage across the globe. In today's world, this cannot be done without laying the critical foundation needed to harness the power of its own data and information systems. This is the realization of cloud computing: the ability to organize, analyze, secure, scale, and ultimately, capitalize on critical information and fight in the digital age. These capabilities must be ubiquitous and available to all Department decision makers, warfighters, and staff.

2.2 Scale for the Episodic Nature of the DoD Mission (Elasticity)

By implementing a scalable solution, mission owners will gain significant efficiencies in the execution of mission capabilities and cyber operations by fully embracing the dynamic elasticity of commercial cloud architecture. The Department's cloud infrastructure will allow for provisioning and deprovisioning of resources automatically. This provides optimum asset utilization when compared to traditional IT infrastructure that is constantly in use, even when demand is minimal. This efficiency will also eventually improve the government's budgeting, billing, and payment practices by providing detailed resource usage reports for all mission owners. This transparency will further drive more efficiencies in the future on how applications are built.

Additionally, the cloud pay-for-use model will provide the flexibility to optimize costs across the IT portfolio and allow DoD to adapt to changing priorities, budgetary conditions, and industry developments. To achieve this cost transparency, strong governance will need to be put in place for how applications are built and data is transmitted and stored. As we develop these standards, implement them, and subsequently learn and better align our services and data to an enterprise solution, we can look to automated tools and techniques to better inform accurate tracking of financial execution of cloud resources.

2.3 Proactively Address Cyber Challenges

DoD must create a standard cloud-based cyber architecture that addresses the needs of commercial and internal-based clouds and encompasses infrastructure, applications, and data. This must include the ability to keep the environment "evergreen" in terms of security and technology.

DoD will produce a unified cybersecurity architecture that addresses cloud and the needs of classified and unclassified missions and data. The capabilities will be tested and assessed independently and frequently to ensure that cybersecurity attributes remain effective against developing threats.

DoD must embrace modern security mechanisms built into modern commercial cloud providers' platforms to ensure the security of these large amounts of data and to safeguard the information. This requires shifting the focus of security from the perimeter edge of the network to actively controlling use of the data itself. In addition to modern encryption algorithms and key management built into commercial cloud services, proper tagging of data will allow for it to be tracked and protected at the necessary levels. DoD will develop a Data Management Strategy that provides the focused discussion with respect to data.

In addition to DoD data security, each Cloud Service Provider will be integral to combating cyber challenges and securing the cloud. The Cloud Service Providers will automatically scan infrastructure resources and generated logs, which will be used to identify vulnerabilities early and to make intrusion detection and mitigation in near-real time a reality across much of the enterprise. With the rise of hardware vulnerabilities, such as Spectre, and increased insider threat, a focus must be applied to both software and hardware—which change at an incredible pace. Keeping up with those changes is difficult, but failure to keep pace has created significant security risks and will only increase in the years to come. Here, again, modern commercial providers have addressed this problem. Moving infrastructure from DoD-managed, on-premises facilities to the cloud will take advantage of the rapid roll out of software and hardware updates. Cloud Service Providers are able to shift workloads within their data centers such that updates are seamless to customers. Hardware with defects or vulnerabilities is constantly swapped out and software patches are applied with vigor in a secure and fault tolerant manner.

Although commercial cloud has many security advantages and opportunities for the Department, the transition to the commercial cloud environment also presents new security challenges. The transition from traditional IT management to the managed cloud service model alters the balance of visibility and control with ease of use, automation, leading edge technology adoption, and optimization of its information domain. The DoD CIO is responsible for defining the security guidelines in the cloud environment. The risk and the responsibility for executing the security in the cloud environment is shared between the Cloud Service Provider(s) and the system owners. DoD CIO will identify the command and control (C2) requirements of the shared cybersecurity responsibility model between DoD and commercial vendors to ensure standard execution of C2 responsibilities for DoD information in commercial cloud. The specific requirements of securing a cloud environment will strain the traditional technical workforce and requires specialized skills where the Department currently has limited expertise.

Historically, information security has been heavily focused on perimeter defense: limiting network access at the boundary. Unfortunately, this model is challenging for a commercial cloud environment where data is being accessed remotely and shared within and between deployments, regions, and from each Cloud Service Provider to other data locations, such as on-premises data centers at military installations. Therefore, the Department will shift its security focus from perimeter defense to securing data and services. This shift will be accomplished first through strong authentication for both people and machines and secure encryption mechanisms both at rest and in transit. In order to facilitate remote access, the DoD cloud environments will supply built-in cryptographic technology that enables organizations to encrypt communications by default. Since the information security responsibility is shared between the Department and its Cloud Service Providers, the Department will include language in all cloud computing contracts directing Cloud Service Providers to monitor their cloud infrastructure and maintain authenticated, encrypted logging of security-relevant events that generate an audit trail and are engineered to be resistant to tampering. To address the workforce strain in adopting these new security postures, the Department will include cloud adoption assistance and specialized training for its workforce as a part of DoD Cloud Service Provider contracts.

2.4 Enable AI and Data Transparency

DoD must enable decision makers to use modern data analytics, such as AI and machine learning (ML), at the speed of relevance to make time-critical decisions rapidly in the field to support lethality and enhanced operational efficiency. The algorithms used to inform decisions are dependent on the Department's data and information being organized, secure, and visible in a common environment. An environment where data is stored in a multitude of disparate and disjointed stove pipes reduces the efficiency and tempo of the Department. To maximize the utility of cloud computing technologies, data must be managed properly and follow modern technologies like data lakes and data hubs, which are accelerated and amplified by cloud technology.

Data stored in an enterprise DoD cloud will be highly available, well-governed, and secure. Data will be the fuel that powers those advanced technologies, such as ML and AI. This critical decision making data will be made available through modern cloud networking, access control, and cross domain solutions to those who require access. Common data standards will be a key part of the Department's methodology for tagging, storing, accessing, and processing information. Ensuring an enterprise cloud environment will increase the transparency of this data, and drive the velocity of data analysis, processing, and decision making. Leveraging advances in commercial cloud security technologies will ensure the Department's information is protected at the appropriate level.

Commercial cloud provides the ability to scale and secure both the collection and the analysis of data stored in an enterprise DoD cloud. This gives mission owners the capability to make decisions with the most relevant information. The distributed nature of cloud computing allows for a more flexible execution environment while simultaneously providing increased information security. This allows for scaling and distributing data repository stores while maintaining security posture and providing new opportunities to obtain mission insights through data collaboration. Similarly, the computing power required for analysis of massive amounts of data can be scaled seamlessly in seconds. This ability to scale will ensure that mission execution is not hindered by insufficient computing and storage capacity and enable the creation of new information models that were previously unachievable.

2.5 Extend Tactical Support for the Warfighter at the Edge

The DoD cloud environment will serve mission owners in every environment, across the range of military operations, from the tactical edge to the home front, both CONUS and OCONUS, and at all classification levels and disseminations (e.g., NOFORN and REL). We must embrace computing solutions that enable warfighters in their environment versus forcing them to conform to the current environment of siloed data and legacy applications. The integration and operation of computing solutions will be straightforward and repeatable, regardless of the required classification level of the system. This will allow warfighters to make data driven decisions and enhance DoD ability to share data with allies and operate as a coalition force. The security of the classified environments will support the level demanded by mission requirements.

Industry has made huge strides in disconnected operations. The Department's General Purpose and Fit For Purpose clouds will capitalize on these efforts to provide the warfighter with the latest technology where they need it and when they need it regardless of the environment. Cloud devices employed by warfighters at the tactical edge will be ruggedized and adaptable, providing for automatic synchronization to the greater cloud once communication is sufficient or reestablished. While certain DoD programs are not immediately amenable to migration to the cloud, some of these sytems may ultimately be bridged to the cloud, while others may be addressed through separate non-cloud solutions. But overall, this auto synchronization of information will ensure warfighters are retaining data, feeding it back into models, and fighting with the most recent algorithms. Doing this in a secure environment will be a force multiplier and directly support the primary goal of the cloud environment: information superiority.

2.6 Take Advantage of Resiliency in the Cloud

Enterprise cloud allows for continuity of operations and efficient failover in times of crisis and operational disruption. Cloud computing is a key component in overcoming these challenges and ensuring comprehensive mission execution, due to its distributed, scalable, and redundant nature. Executing this cloud strategy will incorporate standard approaches to leveraging cloud for this mission resiliency. The enterprise cloud will offer support for failover in times of infrastructure degradation as well as recovery from operational outages and significant cyber incidents.

The distributed, redundant nature of cloud computing overcomes another cyber challenge with its ability to failover in times of crisis. Our commercial cloud solutions will use advances in technology to automate failover, solving a major deficiency throughout the Department. DoD will only be able to ensure continuity of operations for digital services. We will accomplish this by taking advantage of multi-region and multi-availability zone (AZ) architecture, which exists natively within major cloud providers, and pairing this with the effective deployment of secure

Cloud Access Points (CAPs) to cloud-based cybersecurity solutions for increased resilience. DoD cloud architectures will allow for workloads to shift from one AZ or region to another, within a single cloud provider, nearly instantaneously upon detection of the failure of a primary data center. This will be vital in the case of human-made or natural destruction of a large geographic area. The configuration of automated failover is not itself automatic. To fully achieve this capability, applications will need to be re-architected for the cloud. This will allow the Department to bypass the cost and manual effort currently required for the Department to maintain multiple instances of the same data across cloud providers or on-premises data centers, which does not provide the same level of failover as that provided by commercial cloud.

2.7 Drive IT Reform at DoD

The cloud will allow DoD to further consolidate its sprawling data center assets. The Department still has an opportunity to further rationalize and has done significant work to rationalize and reduce data centers. The cloud will provide an opportunity to accelerate and extend those consolidation opportunities, as well as the opportunity to deliver integrated Defensive Cyber Operations (DCO) and achieve efficiencies through rapid deployment of common services. An enterprise cloud perspective will enable more centralized cloud management and a broader availability of security service options for wider cloud adoption by DoD to include those DoD Components with smaller implementation staff.

3 Strategic Approaches and Guiding Principles

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. Technologies such as AI and ML have the potential to fundamentally change the character of war. DoD will embrace an approach that leverages multiple cloud providers who can provide General Purpose and Fit For Purpose clouds. The interoperability of the multi-vendor and multi-cloud environment will be governed by one overarching enterprise cloud strategy. To achieve the objectives outlined above, the Department will pursue a set of guiding principles that will inform future decisions about enterprise clouds: Warfighter First, Cloud Smart-Data Smart, Leveraging Commercial Industry Best Practices, and Creating a Culture Better Suited for Modern Technology Evolution.

3.1 Warfighter First

Throughout the Department's transition to commercial cloud services, it needs to continuously test that cloud solutions are built in a manner that never puts the warfighter and his/her mission at risk. This will require the Department to rigorously red team and challenge itself with independent assessments of the cloud environment and to utilize tactical distributed computing. At all times, DoD needs to ensure that cloud is addressing the needs of improving military lethality. By constantly challenging itself around lethality with red teams, DoD can ensure that the cloud will be positioned to support the challenges of the global environment.

3.2 Cloud Smart-Data Smart

To achieve the objectives outlined above, the Department must pursue a Cloud Smart-Data Smart approach. This approach includes:

- Cloud Smart: One cloud strategy to adopt cloud solutions that streamline transformation and embrace modern capabilities for multiple clouds and missions
- Data Smart: Data transparency and visibility enabled by enterprise infrastructure, application standards, and data tagging.

The Department seeks to leverage the decision making advantages on the battlefield enabled by AI and ML. The Department will best take advantage of these capabilities by executing this succinct, integrated, and adaptive cloud strategy that encompasses multiple clouds and missions across the entire DoD. Systems/applications can be designed with the cloud in mind to simplify adoption and to allow for integration across the Department. Common data and application standards associated with conducting operations in the cloud, such as data normalization/tagging, transport protocols, and interfaces, will be developed to enable and encourage the adoption of enterprise solutions that navigate DoD away from custom, approaches. These standards, combined with the computing power offered by cloud, will allow the Department to function at a tempo never before seen, making informed, analytical decisions at machine speed.

3.3 Leverage Commercial Industry Best Practices

In addition to Cloud Smart-Data Smart, DoD must leverage commercial industry best practices in its approach. This includes:

- Leveraging commercial technology, capability, and innovation whenever possible
- Maximizing competition to ensure that DoD is getting the best technology and value
- Leverage industry open standards and best practices to avoid lock-in and provide maximum flexibility for future cloud advances
- Independently assessing the services delivered to ensure that the data remains secure.

The Department will leverage critical foundational technologies available in commercial cloud computing and storage, to enable innovation wherever possible, while eliminating considerable technical debt and security risk. DoD is positioning itself to get the best value in today's market of cloud computing capabilities to support warfighting and business requirements and to grow capability as industry evolves. In addition, DoD seeks to maximize competition, not only when awarding the pathfinder General Purpose cloud, but also by ensuring access to a variety of Software as a Service (SaaS) capabilities that are complementary to the General Purpose and Fit For Purpose clouds. The Department must take advantage of the advances that American private industry has made. All of this will be built into commercial pricing structures. If DoD can adopt this commercial mindset toward cloud computing, it can incorporate commercial industry lessons learned into future architecture decisions.

3.4 Create a Culture Better Suited for Modern Technology Evolution

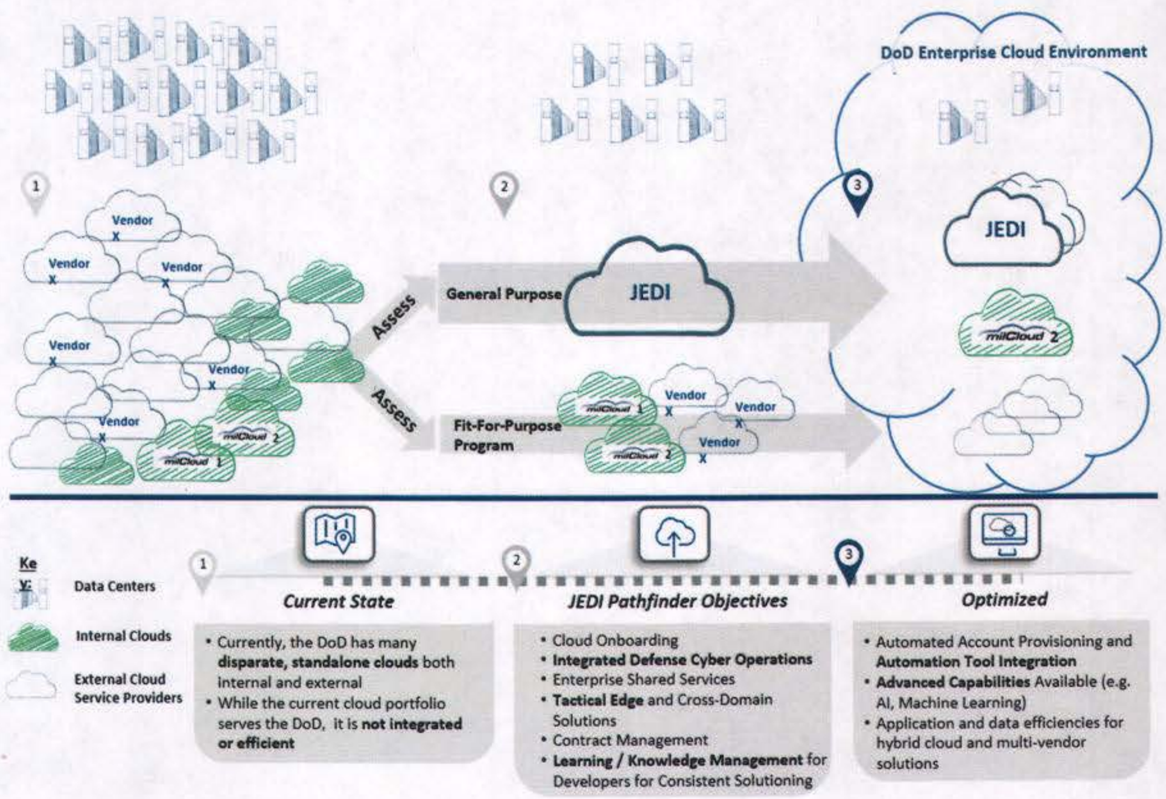
Finally, through this strategy, the Department seeks to create a culture that is better suited for adaptability and modern technology. This includes:

- Creating an environment where people can innovate iteratively
- Embracing enterprise solutions and navigating away from custom federated approaches
- Creating a sustainable culture and workforce that can effectively use what cloud provides
- Creating a culture that enables continuous learning from our cloud partners.

Iterative innovation is essential for successfully adapting modern technologies in an evolutionary fashion. To achieve this, DoD will embrace the use of leading modern technology quickly and more rapid prototyping of new systems. Examples include developing and deploying capabilities for DevSecOps in the cloud environment to securely develop and test software for use in the cloud and using commercial clouds to enable small and medium size companies to more effectively secure Controlled Unclassified Information (CUI). To achieve this innovation and create a culture better suited for adaptability and modern technology, the DoD workforce must change its culture. The Department must develop a cadre of technical professionals, as well as encourage technical proficiency throughout the entire Department. The Department has never built or implemented an enterprise cloud solution and therefore, recognizes the importance of finding a commercial partner to help begin the process of enterprise learning and the development of technical cloud proficiency.

4 Implementation

DoD is driving toward an enterprise cloud environment that is composed of a General Purpose cloud and multiple Fit For Purpose clouds. In addition, it should be recognized that the Department will still need non-cloud data center capability for applications that are not suited for the cloud. Over time, with the adoption of an enduring enterprise cloud strategy, the non-cloud environment should become smaller. There are two fundamental types of work that must be considered in any cloud implementation. The first is a set of fundamental activities that are required to stand up a cloud platform, ready to receive applications, data, or infrastructure for cloud deployment. The second set of activities is the ongoing work to migrate existing applications or to construct new applications onto the cloud platform. Appendix A of this document is a detailed implementation plan that lays out the lines of effort that must be accomplished to fully realize the benefits of cloud computing and to effectively operate on the 21st century battlefield.



Current State

- Currently, the DoD has many **disparate, standalone clouds** both internal and external
- While the current cloud portfolio serves the DoD, it is **not integrated or efficient**

JEDI Pathfinder Objectives

- Cloud Onboarding
- **Integrated Defense Cyber Operations**
- Enterprise Shared Services
- **Tactical Edge** and Cross-Domain Solutions
- Contract Management
- **Learning / Knowledge Management** for Developers for Consistent Solutioning

Optimized

- Automated Account Provisioning and **Automation Tool Integration**
- **Advanced Capabilities** Available (e.g. AI, Machine Learning)
- Application and data efficiencies for hybrid cloud and multi-vendor solutions

Figure 1: DoD Pathfinder to Hybrid Cloud Environments and Multiple Vendors

**JEDI- Joint Enterprise Defense Infrastrucure*

5 Conclusion

Information is a fundamental enabler for advantage on a 21st century battlefield and will enable a more lethal, resilient, and innovative Joint Force. Today, the DoD information environment is made up of multiple disjointed and stove-piped systems distributed across modern and legacy infrastructure around the globe. The data that flows through these systems is growing at an exponential rate. This has caused a litany of problems that impact warfighters', decision makers', and DoD staff's ability to capitalize on critical information to make timely, data-driven decisions. To address these challenges, DoD has implemented a number of cloud solutions; however, they have been built in a disjointed manner. Furthermore, DoD is starting to leverage emerging technologies, such as AI, to help manage the understanding of all the Department's data. However, the critical infrastructure that AI is being built on top of is disparate and disjointed.

To overcome these challenges, DoD will utilize this guiding strategy to further develop a detailed enterprise approach for managing its data, infrastructure, and application landscape. The advent of commercial cloud has provided a powerful opportunity to address these problems. To best take advantage of the opportunity presented by commercial cloud, the Department must implement an enterprise cloud strategy. The appropriate strategy for the DoD will be to leverage a combination of General Purpose and Fit For Purpose clouds along with the advantages of multiple commercial cloud providers. To achieve the objectives outlined above, the Department will pursue a set of interrelated strategic approaches: Warfighter First, Cloud Smart-Data Smart, Leverage Commercial Industry Best Practices, and Create a Culture Better Suited for Modern

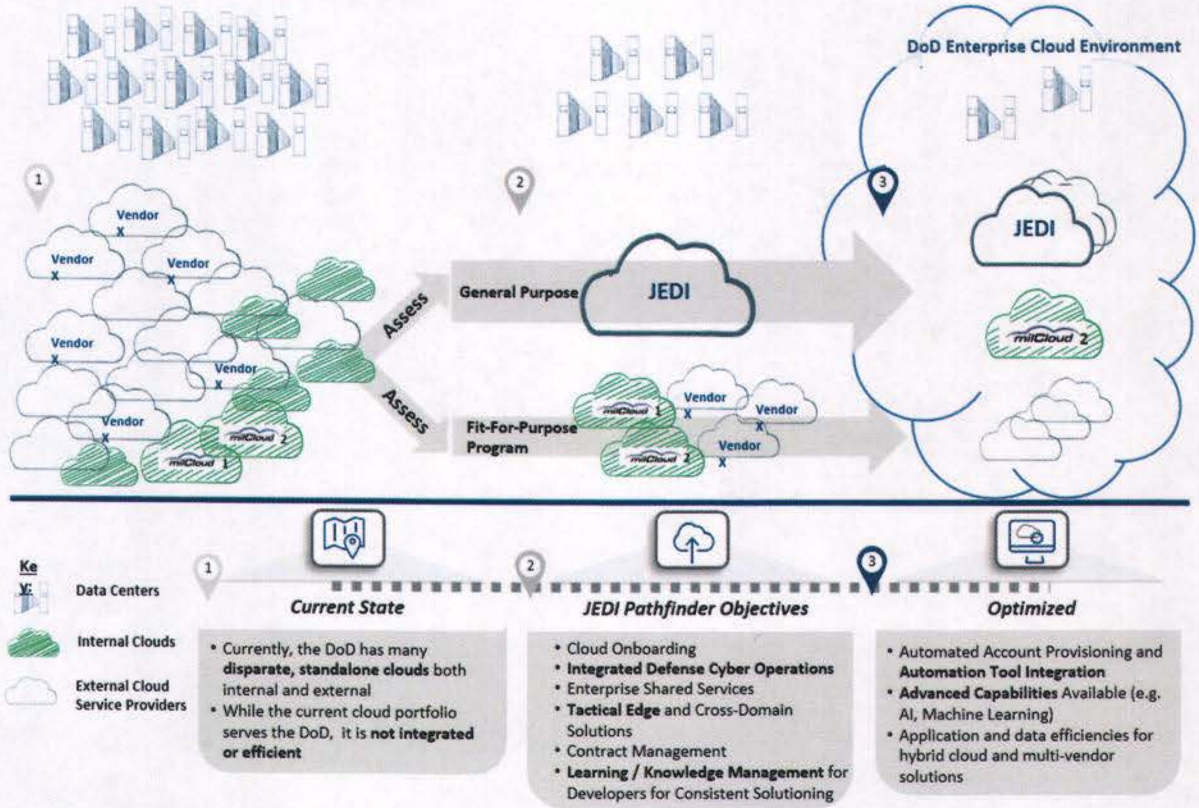
Technology Evolution. DoD needs to develop an organizational construct that insures adoption of the enterprise cloud.

The time is now. DoD can no longer afford to delay its technological and cultural shift to truly modern technologies. Rapidly providing DoD access to underlying foundational technologies, like cloud computing and data storage, on a global scale is critical to national defense and in preparing DoD to fight and win wars. If the Department wants to maintain its overmatch, it will need to leverage technologies such as AI and therefore, it must urgently create an enterprise cloud environment. The strategy outlined in this document provides the approach for moving forward.

Appendix A: Implementation Details

The Department of Defense is driving towards an enterprise cloud environment that is composed of a General Purpose cloud and multiple Fit For Purpose clouds. In addition, it should be recognized that the Department will still need non-cloud data center capability for applications that are not suited for the cloud. Over time, with the adoption of an enduring enterprise cloud strategy, the non-cloud environment should become smaller.

The Department's Enterprise Cloud Environment components and important considerations-migration, governance, and workforce- are described in detail below.



- Currently, the DoD has many **disparate, standalone clouds** both internal and external
- While the current cloud portfolio serves the DoD, it is **not integrated or efficient**

- Cloud Onboarding
- **Integrated Defense Cyber Operations**
- Enterprise Shared Services
- **Tactical Edge** and Cross-Domain Solutions
- Contract Management
- **Learning / Knowledge Management** for Developers for Consistent Solutioning

- Automated Account Provisioning and **Automation Tool Integration**
- **Advanced Capabilities** Available (e.g. AI, Machine Learning)
- Application and data efficiencies for hybrid cloud and multi-vendor solutions

Figure A: DoD Pathfinder to Hybrid Cloud Environments and Multiple Vendors

General Purpose Cloud: Joint Enterprise Defense Infrastructure

The Department will implement a commercial General Purpose enterprise-wide cloud solution, Joint Enterprise Defense Infrastructure (JEDI), for the majority of systems and applications. This General Purpose cloud will allow for the Department to take advantage of economies of scale, broadly provide common core services, and ensure information superiority through data aggregation and analysis.

To implement the Department's General Purpose cloud, an industry partner will be required. The complexity of this endeavor and the Department's lack of large-scale, enterprise, commercial cloud experience means that this partnership is critical to the successful standup of the enterprise General Purpose cloud.

The implementation of General Purpose cloud needs to comprehend four key tenets:

- Offer Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)
- Offer separate environments at all classification levels
- Centralized computing to tactical edge computing for the warfighter
- Enable emerging technologies, such as AI

The JEDI Cloud Program will be the foundational approach to deliver the benefits of a General Purpose enterprise cloud for DoD while embracing the four tenets above. The setup of and migration to the JEDI Cloud requires the steps outlined in the Migration section. A key implementation imperative is that mission owners will be able to rapidly onboard and control their environments, but with common implementation governance supported by a contract.

Fit-for-Purpose

In situations where a General Purpose cloud solution is not capable of supporting mission needs, the Department may use a Fit For Purpose commercial solution or an on-premises cloud solution. Two examples are described here:

1. Software as a Service (SaaS): DoD software applications (e.g., email, chat, collaboration, etc.) over time will migrate to a subscription service where an industry partner will be leveraged for both applications and infrastructure.
2. The Department's milCloud 2.0 environment, a cloud-services product portfolio managed by the Defense Information Systems Agency (DISA), features an integrated suite of capabilities designed to drive agility into the development, deployment, and maintenance of secure DoD applications.

The primary implementation bias for DoD will be to utilize General Purpose cloud computing. Only when mission needs cannot be supported by General Purpose will Fit For Purpose alternatives be explored. In such a case, a mission owner will be required to submit for approval an Exception Brief to the Office of the DoD CIO describing the capability and why the General Purpose cloud service does not support their mission.

As Fit For Purpose solutions are justified, approved, and established, each Fit For Purpose cloud environment will be enacted with enterprise capabilities and scalability in mind. They should still support networking with the General Purpose cloud environment as well as with other Fit For Purpose solutions through modern commercial cloud capabilities for both inter-cloud and cross-domain communication. Secure network peering will allow for data sharing and increased visibility where required.

The Department recognizes that the commercial cloud marketplace will continue to evolve. DoD expects that cloud technology and offerings will continue to 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.

Cloud Migration

There are two fundamental types of work that must be considered in any cloud implementation. The first is a set of fundamental activities that are required to stand up a cloud platform, ready to receive applications, data, or infrastructure for cloud deployment. The second set of activities is the ongoing work to migrate existing applications or to construct new applications onto the cloud platform. The migration activities will need to be overseen by an ongoing governance process that assures security, application development, and data and infrastructure standards.

The fundamental activities required to stand up a cloud environment are composed of five lines of effort:

1. Technical Build – create network connectivity, encryption, data sourcing, and security services (e.g., authentication and ongoing red team engagement) on an enduring basis.
2. Governance – create stakeholder forums, policies, roadmaps, technical standards (architecture and application development), data connectivity standards, resiliency and failover standards, and migration approaches.
3. Automated Provisioning and Billing – automate the ability to quickly provision cloud resources (storage, compute, and application development) and ensure cloud costs are appropriately captured to provide financial transparency.
4. Migration Capability – create repeatable migration process, backed with qualified staff and playbooks for onboarding tenants.
5. Workforce Development – identify, train, and engage resources to create a robust and sustainable cloud workforce.

After the standup of the cloud environment and the conclusion of fundamental activities, the ongoing activities of migrating applications will take over. The magnitude of effort required to stand up a General Purpose cloud at the scale and complexity of the Department is initially best served through a single provider that will allow DoD to maximize pace and minimize risk. The effort required to migrate applications will vary greatly from system to system. Migrating to a cloud environment is not typically as simple as "lift and shift." The migration process will be defined in the DoD's Cloud Migration Playbook and will include the many different paths to realize cloud. The Department will closely monitor the initial efforts to migrate into the Department's General Purpose enterprise cloud. The lessons learned from the various migrations will inform the regular refinement of the playbook, which will provide a consistent and repeatable process for mission owners to apply to their respective systems and applications.

Organizations within DoD that have previously implemented their own cloud will work with the Office of the DoD CIO to determine the best way to integrate their efforts with the Department's enterprise cloud strategy. Where it makes sense that a standalone cloud environment should be migrated to the Department's General Purpose cloud, a thoughtful migration approach will be developed that does not disrupt existing contracts. If it is determined that an existing standalone cloud should be retained, it will be given a formal Fit For Purpose designation and will be expected to adhere to the DoD's enterprise cloud policies.

Governance and Organization

Oversight and governance for the initial build out of this enterprise cloud strategy will be led by the Office of the DoD CIO. At some future date, once the General Purpose cloud environment is fully implemented and Fit For Purpose implementations have matured, it is possible that overall leadership could be transitioned to a different organization inside DoD. The DoD CIO will establish an enterprise cloud organization with appropriate leadership and the required governance forums to ensure that overall objectives and implementation plans as described in this strategy are enacted. The DoD CIO will leverage existing governance forums to the greatest extent possible.

The DoD CIO will organize forums that bring together all lessons learned and find ways to integrate into DoD policies, procedures, and acquisition strategies moving forward. These forums will allow the Department to do regular checks on cloud adoption progress and course correct quickly. The forums will develop detailed implementation plans on rationalization, assessment, planning, and budgeting for accelerating the digital environment to migrate into the enterprise cloud solution.

These forums must be the catalyst to aggressively move the Department to embrace the use of cloud. The DoD CIO in conjunction with the governance forums will provide written guidance on the process and what factors are key to assessing a system for General Purpose or Fit For Purpose hosting. The Department must strive for a Cloud First bias on all future application development/implementations. Organizations should move toward modernization by implementing "cloud native" applications, meaning that the architecture of the system can make use of the scalable, dynamically elastic, distributed nature of cloud computing platforms. Leaving systems running on legacy infrastructure or using other legacy technology must be the exception, not the standard.

Additionally, these forums will work through the Office of the Under Secretary of Defense for Acquisition and Sustainment (A&S) to address current regulations that govern acquisitions to fully take advantage of modern utility/consumption-based services and to enhance contracting capabilities and ATO processes to enable reuse of PaaS/SaaS and cloud-based applications. Working through Cost Assessment and Program Evaluation (CAPE), the forums will provide early insight into annual Planning, Programming, Budgeting, and Execution (PPBE) for cloud activity in the Department. Additionally, these forums will work with the Office of Chief Management Officer (CMO) for application of relevant data standards and governance processes in cloud activities.

As JAIC matures, a key organizational imperative will be to ensure that the requirements of JAIC and enterprise cloud are being jointly integrated.

Workforce Considerations

In today's world, our adversaries are working to develop new capabilities that leverage the advantages of cloud. Therefore, we must ensure, that as we migrate and become more dependent on the cloud, that we are organically growing our cloud technical skills to outpace our adversaries. We can never lose sight that cloud is a key enabler for emerging technologies, such as AI. The future DoD cloud workforce must grow organic technical capabilities by building a more diverse and balanced workforce among military and civilian components. DoD's workforce must obtain a basic level of cloud proficiency in order to most effectively exploit the benefits of cloud. Just as every Marine is a rifleman, every DoD employee must have basic cloud awareness to effectively operate on the 21st century battlefield.