Information Technology Acquisition Advisory Council

# Report to Department of Defense And Congressional Defense Committees

July 2019

# DOD CLOUD ADOPTION

## The Department's Cloud Strategy Sets a Modern Vision for Cloud Adoption, but the Joint Enterprise Defense Infrastructure (JEDI) Request for Proposals (RFP) will not achieve that Vision

IT-Acquisition Advisory Council

Highlights

Why IT-AAC Did This Study

The Information Technology Acquisition Advisory Council (ITAAC) is a public/private partnership of concerned citizens, public interest groups, private sector sponsors and government partners working together to serve as a catalyst for positive change and evolution in the Information Technology Acquisition System to meet the demands of the 21st century. Our mission is to provide Congress, White House, and Executive Branch IT Leadership with a trusted collaborative structure and Transformation Roadmaps for Streamlining the IT Acquisition Process, assuring critical mission elements that are highly dependent on IT (Info Sharing, Cyber-Security, E-Health, E-Gov, E-Biz, and Green IT). The IT-Acquisition Advisory Council is a 501(C)6 Standards Consortium with the participation of transformation minded senior leaders from government, academia, industry and public interests.

This Study Compares the vision set out in the Department of Defense's December 2018 "DOD Cloud Strategy" and the requirements specified in the Joint Enterprise Defense Infrastructure (JEDI) Request for Proposals which was released in July, 2017

The Study finds troubling differences between the stated goals in the DOD Cloud Strategy and the actual requirements in the RFP, which in many areas contradict the Strategy.

# DOD CLOUD ADOPTION

## The Department's Cloud Strategy Sets a Modern Vision for Cloud Adoption, but the Joint Enterprise Defense Infrastructure (JEDI) Request for Proposals (RFP) will not achieve that Vision

**Executive Summary**

The DoD CIO's December 2018 *DoD Cloud Strategy* (Strategy) outlines a compelling vision for cloud adoption within DoD, yet it is fundamentally incompatible with the requirements specified in the Joint Enterprise Defense Infrastructure (JEDI) Request for Proposal (RFP):

- Where the JEDI RFP stipulates a single, static cloud solution, the strategy outlines a rich environment including multiple cloud solutions.
- The Strategy demonstrates a sophisticated understanding of the security challenges facing DoD that is absent from the JEDI RFP.
- The Strategy recognizes the central role that Software as a Service (SaaS) will play in the DoD IT ecosystem, yet SaaS is entirely absent from the JEDI RFP. Instead, the JEDI RFP plans to deploy SaaS through a vendor-managed marketplace with applications hosted on the JEDI cloud, a concept that is not a part of the Strategy and is materially divergent from how SaaS is deployed.
- The JEDI RFP treats cloud at the tactical edge as an integral part of a cloud service and makes no long-term provisions for building out tactical cloud, two technical and architectural mistakes which are not repeated in the Strategy.
- The JEDI RFP imposes strict technical specifications, restricting access to innovative technology, unlike the Strategy's call for DoD to follow the lead of the private sector.
- The Strategy acknowledges important trends in private sector cloud architecture and deployment – including multi-cloud environments, cross-platform interoperability, and cloud migration – that are given no weight in the JEDI RFP.

To address these shortcomings and protect the interests of the Warfighter, the DoD should rescind and revise the JEDI RFP to ensure consistency with the new approach outlined by the strategy. At this point, with the JEDI RFP already released and competition under way, DoD is committed to assessing solutions against criteria that do not match the direction outlined in its Strategy. Without this adjustment, DoD will embark on a $10 billion, ten-year cloud commitment that will not meet warfighting needs, while also creating significant risk to our most sensitive data by exposing it to commercial networks.

# TABLE OF CONTENTS

# IT Acquisition Advisory Council (IT-AAC)

***Recommendations for Restructuring DoD's JEDI Cloud Strategy***

**The Honorable James Inhofe**
Chairman, Senate Armed Service Committee
Committee
Russell Senate Building, Room 228
Washington, DC 20510

**The Honorable Jack Reed**
Ranking Member, Senate Armed Service
Committee
Russell Senate Building, Room 228
Washington, DC 20510

**The Honorable Adam Smith**
Chairman, House Armed Services
Committee
2216 Rayburn House Office Building
Washington, DC 20515

**The Honorable Mac Thornberry**
Ranking Member, House Armed Services
Committee
2216 Rayburn House Building
Washington, DC 20515

**The Honorable Mark Esper, Nominee**
Secretary of Defense
Pentagon
1400 Defense Pentagon
Washington, DC 20301-1400

**Mr. Dana Deasy**
DoD CIO
Pentagon
1400 Defense Pentagon
Washington, DC 20301-1400

**Mr. Chris Liddell**
Director, American Technology Council
The White House
1600 Pennsylvania Ave
Washington DC 20500

**The Honorable Russell Vought**
Acting Director
Office of Management and Budget
725 17th Street, NW
Washington DC 2050

July 23, 2019

**Dear Defense Secretary Nominee Esper, Senator Inhofe, Senator Reed, Representative Smith, Representative Thornberry, Director Vought, Mr. Liddell, and Mr. Deasy,**

With a federal court removing the last remaining challenge to awarding the DoD JEDI contract, we at the IT-AAC would like to share our concerns with the JEDI cloud program and the national security implications of moving forward with a program that undermines implementation of industry best practices.

As such, detailed in the attached report, "DOD CLOUD ADOPTION: The Department's Cloud Strategy Sets a Modern Vision for Cloud Adoption, but the Joint Enterprise Defense Infrastructure (JEDI) Request for Proposals (RFP) will not achieve that Vision" we once again offer recommendations on how to realign

the DoD JEDI RFP with the forward thinking found in the DoD Cloud Strategy, OMB's Cloud Smart Policy, and EO 13800.

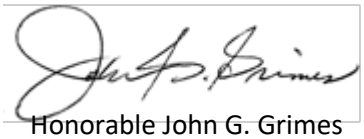
As the nation's leading voice on Federal IT Reform, we applaud DoD's effort to usher in commercial cloud innovations and standards of practice emanating from Fortune 500 and industry leaders. However, we believe a better outcome would come from a multi-cloud approach as detailed in the DOD Cloud Strategy that includes continuous updates and expansion of MilCloud to house our most sensitive data, and adoption of commercial cloud, hybrid, and private cloud across the department to enable IT Modernization across multiple architectures, and enable modern technologies such as Artificial Intelligence (AI).

The IT-Acquisition Advisory Council (IT-AAC), a federation of two dozen leading IT industry groups (NGO) and Standards Bodies (SDO), was chartered in late 2007 to provide leaders from Congress, the White House and the Executive Branch alternative sources of expertise and insights that are more representative of the $4 trillion Global IT market, of which Federal IT sector is less than 2%.

Since the beginning of the government's journey into the cloud, the IT-AAC has provided objective and evidence-based insights to Congress, the White House and Executive Branch that have directly impacted key policy initiatives (FITARA, EO13800, Cloud First, Cloud Smart, DoD Cloud Strategy). Having closely monitored the JEDI strategy since its inception, we believe there are some critical gaps that must be addressed to avoid putting our national security mission at risk. Please find below our concerns and recommendations for realignment of the JEDI cloud procurement.

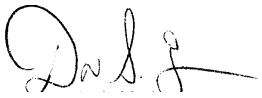
Very Respectfully,

Honorable Duane Andrews
Former DOD CIO/ASD C3I

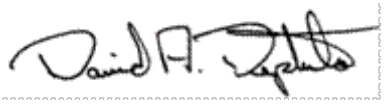


Honorable John G. Grimes
Former DoD CIO

Dr. Marv Langston
Former DOD CIO



Honorable Dov Zakheim
Former USD (Comptroller)



Dave Deptula, LTG USAF Ret
Dean, Mitchell Institute

Tony Scott
Former Federal CIO

Kevin Green, VADM (ret)
Former Deputy CNO

Steve Cooper
Former CIO; DHS, FAA, Commerce

Ken Deutsch, RADM, USN (Ret)
Former EVP CSRA Defense Group

# JEDI INTRODUCTION

The JEDI RFP was a result of the work of the Cloud Executive Steering Group (CESG), established by Deputy Secretary Shanahan in a September 13, 2017 memo[1]. The memo recognized the realities of the changing nature of warfare and that the DoD was falling behind in embracing and utilizing modern Information Technology. Specifically, the memo stated:

1. Technologies in areas like data infrastructure and management, cybersecurity, and machine learning are changing the character of war;
2. Commercial companies are pioneering technologies in these areas; and
3. The pace of innovation is extremely rapid.

The memo then directed the Director of the Defense Digital Service (DDS) to "use a tailored acquisition process to acquire a modern enterprise cloud services solution that can support unclassified, secret, and top-secret information." As a result, DoD released a Request for Information (RFI) in October 2017[2], a draft RFP in March 2018[3], a second draft RFP in April 2018[4], and a final RFP on July 26, 2018[5] for the JEDI cloud.

While JEDI was intended to be a part of a larger DoD cloud environment, the vision for this larger environment was not articulated until the DoD Cloud Strategy was publicly unveiled in February, 2019[6]. The Strategy took a different direction from the JEDI RFP, embracing multi-cloud, hybrid, and commercial cloud solutions. Unlike JEDI, the Strategy integrated lessons from private sector use of cloud services and explained how DoD would transition from legacy on-premises systems to a modern cloud architecture. It also dictated how DoD would use SaaS in conjunction with other cloud architectures. The net result is that the JEDI RFP and the DoD Cloud Strategy articulate different, incompatible approaches to cloud adoption across DoD.

[1] https://www.nextgov.com/media/gbc/docs/pdfs_edit/090518cloud2ng.pdf
[2] DOD Cloud: Request for Information, Solicitation Number: DOD_Cloud_RFI, https://www.fbo.gov/index?s=opportunity&mode=form&id=6fe635bc817ad6913c405d25ec5a34b5&tab=core&_cview=1
[3] DRAFT DOD JEDI Cloud RFP, Solicitation Number: HQ003418R0077-JEDI_Cloud_DRAFT_RFP, https://www.fbo.gov/index?s=opportunity&mode=form&id=f7f1d0314ec7c83cd0ace1636b5474a1&tab=core&_cview=0
[4] DRAFT DOD JEDI Cloud RFP, Solicitation Number: HQ003418R0077-JEDI_Cloud_DRAFT_RFP, https://www.fbo.gov/index?tab=documents&tabmode=form&subtab=core&tabid=bad7eaa1135691af5d7963995f69ee22
[5] JEDI Cloud RFP, Solicitation Number: HQ003418R0077_JEDI_CLOUD_RFP, https://www.fbo.gov/index?s=opportunity&mode=form&id=7a17a56421e2d84e53c8ee6f7209ef8f&tab=core&_cview=0
[6] Mitchell, Billy, "DOD unveils enterprise cloud strategy with preference for JEDI cloud" fedscoop, Feb 4, 2019, https://www.fedscoop.com/dod-cloud-strategy-unveiled-congress/

## THE CHALLENGE OF JEDI

The JEDI RFP was developed without the Strategy as a guidepost. As a result, the content presented at JEDI Industry Day, in the responses to the thousands of questions submitted to DoD, and in the JEDI RFP itself has committed the DoD to selection criteria that are in direct conflict with the Strategy. While the Strategy describes JEDI as one part of a complex environment, the JEDI RFP approaches JEDI as an isolated system. Furthermore, the Strategy requests many features that are assessed and scored nowhere in JEDI. Unless DoD acts immediately, the Strategy will produce neither the desired results nor a modern cloud architecture. Instead, the limitations in JEDI will limit DoD's ability to embrace a modern multi-cloud environment and protect its most important information assets from being compromised.

## PROCUREMENT AND LEGAL CONSTRAINTS

DoD is legally constrained by the terms of the current JEDI RFP. Under Federal Acquisition Regulation (FAR) rules, DoD must score and award JEDI based on the requirements specified in the RFP. Deviating from these requirements will open DoD to protests and legal challenges that will kill a core piece of its cloud adoption strategy. The only solution that will align the Strategy and JEDI is amending the solicitation, permitting all major commercial cloud suppliers to submit proposals for services DoD says it needs.

DoD has a "fundamental obligation to conduct a competition on the basis of the most accurate or realistic estimates" regarding its needs for cloud services.[7] Because the Strategy is intended to inform Congress how DoD will implement cloud computing, it must be viewed as the most accurate statement of what DoD intends to procure.[8] Yet in comparing the Strategy and the JEDI RFP, it is clear DoD cloud services needs have changed since the RFP was issued. The FAR states "[w]hen, either before or after receipt of proposals, the Government changes its requirements or terms and conditions, the contracting officer shall amend the solicitation."[9] As a result, DoD must amend the JEDI RFP to accurately reflect DoD needs under its Strategy, allowing offerors to submit new proposals that address those needs.

[7] DZSP 21, LLC v. United States, 139 Fed. Cl. 110, 117 (2018)
[8] See FY19 NDAA § 1064 (requiring DoD to report to Congress on its Cloud implementation strategy).
[9] 48 C.F.R. § 15.206(a); see also DZSP 21, 46 Fed. Cl. at 117 (Section 15.206(a)'s "mandate is triggered '[w]hen ... the [g]overnment changes its requirements' and is stated in categorical terms—the government 'shall amend the solicitation.'") (alterations and emphasis in original); MVM, Inc. v. United States, 46 Fed. Cl. 126, 131 (2000) (recognizing that a material change in the scope of the government's needs requires an amendment of the solicitation).

The only way to change evaluation criteria is through an amended RFP. DoD may not evaluate existing proposals under criteria other than those stated in the JEDI RFP.[10] Furthermore, it may not use the JEDI contract to procure the materially different services envisioned in the Strategy. Under the Competition in Contracting Act (CICA), doing so would "circumvent the statutory requirement for competition."[11] It would also contradict DoD's sole-source justification[12], which required DoD to assert that JEDI will involve only "Firm Fixed-Price task or delivery orders for services for which prices are established in the contract for the specific tasks to be performed." Adding new services post-award would be a cardinal change, which is unlawful under CICA and the statutory prohibition on single award IDIQ contracts over $112 million.[13] Each such change in contract scope would be a protestable event, causing the delay and burden DoD claims it wants to avoid.[14] Amending the JEDI RFP now will allow DoD to comply with the law and avoid administrative work and protests that will delay DoD implementation of its Strategy, precisely what DoD claims is a paramount concern.

The Intelligence Community has already encountered a similar situation with the Cloud Computing Services (C2S) contract. After the contract award, IBM filed a protest against the decision to award the contract to Amazon, which was upheld by the Government Accountability Office (GAO). This led to a second protest by Amazon, citing the government's response to the GAO's ruling as "overbroad, unreasonable, and in violation of federal law and regulation." The issue was ultimately settled in court, forcing the CIA to stick to its earlier, incomplete criteria. The impact has been an environment that continues to fall short of the Intelligence Community's needs.

[10] Banknote Corp. of Am., Inc. v. United States, 56 Fed. Cl. 377, 385 (2003) ("It is hornbook law that agencies must evaluate proposals and make awards based on the criteria stated in the solicitation. This requirement is firmly rooted in the Competition in Contracting Act (CICA) … which indicate[s] that an agency shall evaluate competitive proposals and assess their qualities based solely on the factors and subfactors specified in the solicitation.") (citing 10 U.S.C. § 2305(a)(2)(A)); Femme Comp, Inc. v. United States, 83 Fed. Cl. 704, 728 (2008) ("An agency's final award decision must 'be based on a comparative assessment of proposals against all source selection criteria in the solicitation.'") (quoting 48 C.F.R. § 15.308).

[11] AT&T Commc'ns, Inc. v. Wiltel, Inc., 1 F.3d 1201, 1205 (Fed. Cir. 1993).

[12] JEDI_Single_Award_DF-USD(AS)_17July18.pdf

[13] See 10 U.S.C. § 2304a(d)(3); 48 C.F.R. § 16.504(c)(1)(ii)(D)(1)(ii).

[14] See, e.g., Northrop Grumman Corp. v. United States, 50 Fed. Cl. 443, 465 (2001) (modification of a contract "outside the reasonable expectations of the bidders" requires competition and failure to open to competitive bidding is a protestable event).

# WHY JEDI DOESN'T WORK FOR THE WARFIGHTER

The JEDI RFP fails to include many features that DoD requires. The Strategy presents a comprehensive picture of how DoD expects to move to the cloud and describes the evolving DoD ecosystem. It calls for a "multi-cloud, multi-vendor strategy," with the ability to support exponential growth, episodic bursts of activity, thwarting cyber threats, artificial intelligence, data transparency, the tactical edge, and resilience. In particular, the Strategy clarifies its vision around several key topics – cloud security, SaaS, the tactical edge, plans to leverage private sector innovation, and classified cloud. Yet these factors appear nowhere in the JEDI RFP.

## REASON 1 - JEDI AS MONOLITHIC CLOUD

The JEDI RFP is focused on a single, sole-source, static system with no consideration for interconnection with other types of systems, while the Strategy envisions a dynamic, multi-vendor, multi-technology environment. For example, in the introduction to the Statement of Objectives, the RFP states that "DoD requires an extensible and secure cloud environment." DoD is pursuing JEDI as a move towards "a general purpose cloud capable of delivering infrastructure and platform services for the bulk of the Department's mission." In viewing JEDI as a singular entity, DoD fails to account for the numerous points of connection that the operational system will require with MilCloud, "Fit-for-Purpose" clouds, on-premises systems, and other IT environments. The JEDI RFP only addresses connectivity in the context of support for open source software and support – specifically, focusing on migration *out* of JEDI, rather than migration *in* or connectivity *across* platforms. As a result, the RFP does not award points for a variety of features that would be valuable in realizing the Strategy. This includes the ability to operate in a multi-cloud environment; cross-platform interoperability; and consideration for migration.

## REASON 2 – SECURITY

The Strategy demonstrates a sophisticated understanding of the security challenges facing a cloud environment. The Strategy suggests DoD must "embrace modern security mechanisms built into modern commercial cloud…shifting the focus of security from the perimeter edge of the network to actively controlling the data itself." It states "with the rise of hardware vulnerabilities…a focus must be applied to…hardware," calling attention to vulnerabilities such as Spectre and Meltdown. It also highlights challenges such as insider threat, which requires fine-grained control over access to data. The "rapid roll out of software and hardware updates" is cited as support for cloud migration. It says DoD will apply advanced technologies like AI to "automatically scan infrastructure resources and generated

logs, which will be used to identify vulnerabilities early and make intrusion detection and mitigation in near-real time a reality across much of the enterprise." All these are correctly highlighted as advanced capabilities that the private sector is developing and deploying at a faster rate than government.

This stands in direct contrast to the JEDI RFP, which focuses on the most basic compliance measures. The second gating criteria for the proposal is built around compliance with existing Federal security regimes such as FedRAMP, which are largely backward-looking standards intended to help cloud vendors integrate with current, lowest-common-denominator Federal IT standards. Of the main assessment factors, only two of nine focus on security. Even these are basic, assessing physical and logical separation (Factor 2) and basic information security and access controls such as audits, logging, and rule based access controls (Factor 4). These approaches are largely perimeter and management based and have little relevance to DoD's vision – and needs – for the most advanced commercial technologies. The only mention of advanced capabilities is near the end of the JEDI RFP Statement of Objectives, which asks for "Advanced automated security capabilities, for example, the ability to detect and respond to adversaries through artificial intelligence." Even this is nowhere reflected in the technical assessment criteria. The net result is a proposal that provides much greater weight to backward-looking security controls. This forced vendors to weight their proposals towards describing their ability to provide lowest-common-denominator security features. Scoring for data-level security, as well as forward-looking investments like automated patching and traffic analysis, are not assessed or scored in the RFP.

## REASON 3 - SOFTWARE-AS-A-SERVICE

The Strategy describes a DoD IT ecosystem where SaaS plays a central role. It begins by acknowledging how and why industry provides these products. It describes a cloud environment that extends beyond Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS), using SaaS to leverage "industry partner[s]…for both applications and infrastructure." Its vision of "Fit-for-Purpose" clouds is a forward-looking approach, as most DoD computing workloads can be best serviced by commercial SaaS applications. For example, enterprise shared services like "email, chat and collaboration" will eventually be significant parts of DoD's cloud ecosystem. DoD is already planning to invest $8 billion in such an environment through the Defense Enterprise Office Solutions (DEOS) contract[15], which had a request for quotations (RFQ) issued on April 26. DoD and the Services will undoubtedly pursue similar cloud contracts for common business systems such as enterprise resource planning, human capital management, customer relationship management, and supply chain management, which will each run on its own infrastructure.

[15] Defense Enterprise Office Solution (DEOS), Solicitation Number: 47QTCA-19-Q-0001, https://www.fbo.gov/index?s=opportunity&mode=form&id=5244dbfda804d301d2e3aba5b8d46c1e&tab=core&_cview=1

Although DoD is clearly envisioning an environment integrating cloud products from many vendors, the JEDI RFP does not reflects this. It actively discourages this vision by making a Commercial Cloud Offering marketplace as a gate criteria (Sub-Factor 1.6), giving the impression it expects SaaS to be run atop the basic JEDI IaaS and PaaS services. The JEDI marketplace, which is a central feature of the RFP, appears nowhere in the Strategy. In fact, the marketplace requirement is the only nod to SaaS in the JEDI RFP. Yet this "marketplace" approach is out of step with both the Strategy and the general market for SaaS. As the Strategy rightly points out, integration of SaaS with other cloud applications will reduce costs, increase performance, and streamline security in DoD's future multi-cloud environment. Yet under the current JEDI RFP, DoD is not allowed to consider the value that this would bring to its enterprise.

## REASON 4 - TACTICAL EDGE

The Strategy realizes that connectivity at the tactical edge is a distinct capability from the commercial public cloud. It rightly identifies data storage and transfer as the main challenge for locations with limited or intermittent connectivity, stating that "auto synchronization of information will ensure warfighters are retaining data, feeding it back into models, and fighting with the most recent algorithms." In doing so, it recognizes that tactical edge is a distinct element of DoD's emerging IT infrastructure, connected to yet separate from the cloud workloads that will process that data. It also acknowledges that "industry has made huge strides in disconnected operations" and that the private sector is leading the way.

However, the JEDI RFP treats connectivity at the tactical edge as an integrated part of the solicited commercial public cloud. While many experts have argued that JEDI requirements for portable, remote, ruggedized compute and storage are not part of standard commercial public cloud, it nevertheless requires these services as an integral part of each vendor's offering. On the other hand, the Strategy states that "the integration and operation of computing solutions will be straightforward and repeatable," out to the tactical edge. This suggests that the Strategy foresees an IT environment that is supported by multiple vendors and systems, all working together. Unfortunately, JEDI offers vendors no flexibility in how they provide connectivity to the tactical edge, instead insisting that it should be an integral part of the cloud service offering.

## REASON 5 - HARNESSING PRIVATE SECTOR INNOVATION

The Strategy calls for DoD to follow the lead of the private sector, putting the mission first, and building cloud solutions around the needs of the warfighter. In doing so, it aligns with the approach outlined in the Office of Management and Budget's "Cloud Smart" strategy published this fall. Indeed, it explicitly

calls for a Cloud Smart approach. Additionally, it says DoD "seeks to maximize competition" and that it must "take advantage of the advances that American private industry has made." It further recognizes that this is built into existing commercial pricing structures and that DoD must "adopt this commercial mindset towards cloud computing." In numerous places, the Strategy highlights how the private sector has solved problems that continue to bedevil the public sector, such as development of innovative security capabilities and application of cost-effective, general purpose software applications.

This stands in stark contrast to the JEDI proposal, which contains highly detailed technical requirements. Indeed, during the JEDI Industry Day, one speaker highlighted this as a key feature of the procurement and process. In doing so, the JEDI RFP limited vendors' ability to educate the government on current industry best practice and the ways in which their solutions address known problems with cloud adoption, migration, and operation. Multiple cloud vendors have invested heavily in developing autonomous cloud management capabilities and in simplifying migration in response to the challenges large enterprises have had in moving into the cloud. Yet JEDI does not consider these innovations, which would have provided significant additional value to the government.

## REASON 6 - CLASSIFIED CLOUD

The Strategy clearly illustrated a long-term, enterprise wide commitment to providing the same suite of services at all classifications. It discusses the need for an environment that serves "mission owners" at "all classifications levels and disseminations (e.g., NOFORN and REL)." It clearly pushes back on "the current environment of siloed data and legacy applications." In doing so, it is making a bold commitment to ensuring every part of the cloud infrastructure will support both classified and unclassified environments. Given its commitment to a multi-vendor environment, this will clearly mean supporting multiple vendors in building out unique, classified environments that will primarily serve DoD. This large investment in infrastructure is the only way to realize the broadly interconnected vision that DoD has laid out.

However, JEDI makes no provision for this long-term effort to build out classified cloud environments. It requires an exceptionally rapid build-out for Impact Level 5 (IL-5), secret, and top secret environments for JEDI as a factor in its procurement. In doing so, it weights the competition towards vendors that have already built classified environments using older technology. Given that DoD is committing itself to the long-term build-out of classified environments, it is baffling that JEDI would use short timelines. It is critical for DoD to make a commitment to expanding and upgrading classified environments on an on-going basis, rather than relying on dated, or even current, security criteria.

## REASON 7 - MULTI-CLOUD ENVIRONMENTS

The Strategy acknowledges that the DoD will need a computing ecosystem where the warfighter can choose the right system for the mission. It says DoD will "embrace an approach that leverages multiple cloud providers who can provide General Purpose and Fit for Purpose clouds," creating the varied ecosystem needed to address DoD's varied missions. It further aligns with OMB's 2018 Cloud Smart strategy, calling for a "Cloud Smart-Data Smart" approach that includes "embracing capabilities for multiple clouds and missions." A vision that will include general cloud infrastructure alongside tailored, cloud-hosted platforms and software recognizes that DoD will be working in a multi-vendor, multi-product environment. Furthermore, the vision of "Fit for Purpose" clouds appropriately recognizes that vendors differentiate their products to meet the needs of a varied market. In Appendix A, DoD demonstrates a vision for a DoD Enterprise Environment that includes commercial public cloud (JEDI), private cloud (MilCloud), and "Fit-for-Purpose" solutions that include SaaS which provide "application and data efficiencies for hybrid cloud and multi-vendor solutions."

This is in stark contrast to the JEDI RFP, whose focus on a single-vendor award downplayed the importance of features that permit integration and deployment across many types of environments. At $10 billion over 10 years, JEDI envisions a DoD enterprise environment that will be homogenous and dominated by a single vendor's architecture. Until the release of the Cloud Strategy, all indications were that DoD was looking for a single vendor to handle the vast majority of its workloads. The JEDI RFP stated, "JEDI Cloud is an important first step to acquiring a general purpose cloud capable of delivering infrastructure and platform services for the bulk of the Department's mission."[16]As recently as September 24, 2018, the JEDI contracting office reaffirmed this, stating that the "goal for the JEDI cloud is to encompass 80 percent of current DoD applications."[17] It clearly sought a single-vendor solution and awarded no points for full stack offerings that could deploy across multiple environment. By only assessing a vendor's capability to provide scaled, commercial, public IaaS and PaaS, the DoD orientation precluded Cloud Service Providers from partnering to provide more dynamic solutions and multiple architectures.

[16] JEDI RFP Statement of Objectives, Amendment 1, p. 1
[17] GAO Decision in the Matter of Oracle America, Inc. Protest over RFP HQ-0034-18-R-0077, Nov. 24, 2018, p. 12

## REASON 8 - CROSS-PLATFORM INTEROPERABILITY

The Strategy recognizes that interoperability will occur at multiple levels of the IT stack. It highlights the need to promote "interoperability" through the use of standardized approaches for vendors and clouds (p. 7), applications (p. 8), and data (p. 4). It discusses steps such as a common lexicon for data tagging and simplifying migration across environments through "leveraging open standards." These steps will help DoD unlock the potential of its data, which "are differentiators to ensure mission success." The Strategy also highlights the need for "strong governance for how applications are built and data is transmitted and stored," emphasizing the broader work that must be done to enable systems and data to interconnect. DoD is clearly planning for a long-term environment where workloads will port between different deployment models, cloud service levels, and vendors. Furthermore, it is obviously looking to ensure it is never overly dependent on a single cloud vendor.

However, in the JEDI proposal, DoD gives no weight to features that promote interoperability across systems, deployments, and vendors. Although DoD seeks to interconnect its systems at multiple layers, the word "interoperability" appears only twice in the entire 99 page proposal – both in the context of data and application portability. Nowhere does it address the immense challenges of cross-connecting different IT environments, applications, and data or ask about tools that will assist this process. The ability to pool data and systems is clearly important to DoD's view of the value that a cloud will bring. It is at the root of DoD's highly controversial decision to award JEDI to a single vendor, as articulated in its May 2018 report. In it, DoD states "use of multiple clouds would inhibit pooling data in a single cloud (i.e. a "data lake).[18]" Yet the JEDI RFP never asks about tools that will enable this high level objective. Because DoD failed to acknowledge its broader efforts to cross-connect applications and data, vendors cannot receive credit for the value of integrated cloud platforms and connectivity to software and hardware installed across DoD.

## REASON 9 - CONSIDERATION FOR MIGRATION

The Strategy draws attention to the challenges of migration. Up-front, the Strategy states that one of the Strategy's fundamental focuses is "the ongoing work to migrate existing applications" to the cloud. Later, the Strategy highlights JEDI as part of the process of transitioning from the present to a future environment. In doing so, DoD will need to determine which workloads to move and how to move them. As the Strategy states, "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.'" Indeed, it plans to manage this process through a "Cloud Migration Playbook" that will "include many different paths to

[18] Serbu, Jared, "Pentagon: Need for speed justifies single-award approach to JEDI cloud contract" Federal News Network, May 15, 2018

the cloud." Given that a well-planned migration can be the difference between success and failure in a cloud computing project, both in terms of cost and performance, DoD is wise to plan ahead.

In contrast, the JEDI RFP completely fails to consider the challenges of migration. Despite including detailed requirements around issues like commerciality, scale, marketplace offerings, and access control, the RFP contains no assessment criteria related to migration. The only place it comes close are its requirements for vendors to develop a plan to migrate data and applications out of the cloud out of concern over vendor lock-in. The JEDI RFP only scores features that are valuable for new, cloud-native development, yet the Strategy clearly shows that DoD expects to migrate many workloads into this environment. The suites of migration tools and technical architectures that are purpose-built to facilitate the migration of enterprise-scale systems are awarded no consideration in the RFP.

## REASON 10 – JEDI MARKETPLACE

One notable omission from the Strategy is the commercial cloud marketplace envisioned under JEDI. In the JEDI RFP, DoD clearly envisions a cloud computing environment where PaaS and SaaS offerings will be provisioned through the JEDI environment. The Statement of Objectives states that vendors must, "provide the ability to rapidly and securely deploy CSP and third-party platform and software service offerings from an online marketplace." The RFP requires that vendors, "demonstrate that the existing CCO [Commercial Cloud Offering] includes an easy to use online marketplace (via web-accessible user interface) to deploy CCO and third-party platform and software service offerings onto the CCO infrastructure" as part of Sub-factor 1.6, a gate criteria which vendors must comply before their proposal can even be evaluated. Overall, JEDI makes it clear that DoD views the JEDI marketplace as a significant – potentially even primary – way that it will obtain third-party SaaS and PaaS offerings.

However, this marketplace appears nowhere in the DoD Cloud Strategy. In fact, the word "marketplace" appears just once in that document – and in a completely different context. If JEDI is to be the main cloud environment for DoD, this marketplace must be a central part of the Strategy. It should eventually become a major – if not primary – way that DoD accesses commercial cloud products. The fact that it is entirely absent from any diagram of the future DoD cloud ecosystem, and not mentioned once in the Strategy, is a telling shift. When taken with the explicit call-out of SaaS as part of a "Fit-for-Purpose" cloud, DoD has clearly jettisoned a major part of the JEDI vision in the more recent Strategy, bringing it into line with commercial best practices.

## CONCLUSION: CLOUD SMART OR CLOUD RIGHT NOW

DoD stands at a critical juncture. DoD and the warfighter deserve the best capability industry can offer. While the JEDI RFP has been issued, it has yet to be awarded. DoD has not yet made rash investments or committed itself to a multi-year contract obligation. More importantly it has not wasted time that it does not have. DoD still has the opportunity to pause, evaluate, and align its investments with its current strategy. However, unless DoD acts quickly, this opportunity will be lost. By withdrawing and reviewing the JEDI RFP, DoD has the opportunity to benefit from the best that industry can offer now. The DoD Cloud Strategy has set the vision for IT modernization and made the move to the cloud clear. Yet the JEDI RFP undermines the entire strategy by limiting access to innovation; requiring a static cloud environment without on-ramps for new providers and technologies; and failing to recognize the role of SaaS.

# ABOUT IT-AAC

The Information Technology Acquisition Advisory Council (ITAAC) is a public/private partnership of concerned citizens, public interest groups, private sector sponsors and government partners working together **to serve as a catalyst for positive change and evolution in the Information Technology Acquisition System to meet the demands of the 21st century.**

Our mission is to provide Congress, White House, and Executive Branch IT Leadership with a trusted collaborative structure and Transformation Roadmaps for Streamlining the IT Acquisition Process, assuring critical mission elements that are highly dependent on IT (Info Sharing, Cyber-Security, E-Health, E-Gov, E-Biz, and Green IT). The IT-Acquisition Advisory Council is a 501(C)6 Standards Consortium with the participation of transformation minded senior leaders from government, academia, industry and public interests:

- **Government:** CONGRESS- Armed Service, Homeland Security, and Permanent Select Committee on Intelligence. FEDERAL AGENCY – VA, OSD Health Affairs, Navy and Airforce, GSA FAS, Army, White House, NSA, OSD ATL, DHS, and many others.
- **Academia/Public Interest** Harvard KSG, University of Maryland, MIT SLOAN, NDA, CMU SEI, DAU, BENS.org, HIMSS.org, NCOIC.org, CCIA.org, TheCGP.org, ICHnet.org, Aerospace Corp.
- **Industry:** Trusted Computer Solutions, McKinsey, CGI, Accenture, Keane, Microsoft, Google, HP/EDS, nationally recognized IT experts and former government officials.

## OTHER IT-AAC PUBLICATIONS:

- 2009 Roadmap for Sustainable IT Reform Vol1; http://www.it-aac.org/images/ITAACRoadmapCongSumv1.pdf
- 2011 Roadmap Vol 2: http://www.it-aac.org/images/Dec2010Roadmap_Summary.pdf
- 2014 HASC/SASC Response leading to FITARA adoption: http://www.it-aac.org/images/IT-AAC_Defense_IT-Reform_Roadmapv2.0_SignedFinal9-24.pdf
- 2015 FITARA Implementation Roadmap; http://www.it-aac.org/images/IT-AAC_FITARA_Cyber_Roadmap_OMB_SUM.pdf

IT Acquisition Advisory Council
904 Clifton Drive
Alexandria, Virginia 22308
www.IT-AAC.org 703-768-0400 bob.dix@IT-AAC.org