November 17, 2017

The Honorable Ellen Lord  
Office of the Under Secretary of Defense  
Acquisition, Technology, and Logistics (USD AT&L)  
3010 Defense Pentagon  
Room 3E1010  
Washington, D.C. 20301-301

Subject: Accelerating Enterprise Cloud Adoption/DOD Cloud RFI

Dear Mrs. Lord:

On behalf of the members of the IT Alliance for Public Sector (ITAPS),¹ we are writing to provide feedback about the Department of Defense’s approach to accelerating enterprise cloud adoption. ITAPS has long advocated for the Department to migrate many functions to the cloud in order to help modernize DOD’s systems, improve security, increase energy efficiency, and reduce cost. We are encouraged to see the Department take the necessary steps toward this end. We strongly support DoD’s focus on commercial capabilities and solutions to meet its cloud needs. We are concerned with reports regarding a single-award cloud contract for the Department Enterprise, as well as possibly cancelling all awarded DOD cloud contracts leaving the Department with only one cloud solution. Given the significant investment and effort that has gone into existing cloud contracts already in place across a wide variety of DOD agencies, we offer the following comments on the DOD Cloud Request for Information (RFI) issued by the Cloud Executive Steering Group (CSEG).

The Department will greatly benefit from accelerating cloud adoption across the DOD enterprise. We recommend that DOD consider pursuing a strategy utilizing multiple suppliers so that the Department has resiliency and full access to the wide range of technical innovations developed in the commercial marketplace, increasing both functionality and security while reducing costs through competition. A Department cloud comprised of multiple interoperable offerings would ensure that the Department obtains the benefits of competition to achieve best value for both warfighter and taxpayer. In fact, almost all Fortune 500 counterparts have established multi-cloud architectures because no singular cloud solution meets all of their mission and business application requirements. This model of operation would also allow for the inclusion of a host of cloud adoption support services delivered independently of the cloud service providers (CSP’s) that would reduce the risk and time associated with cloud migration. At the same time, cross-cloud services will be required to automate the discovery, metering, management, and provisioning of the workloads to support

¹ About ITAPS. ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter @ITAlliancePS.
their applications across multiple cloud providers. As agencies move into the cloud, the ability to guarantee consistent services, such as cybersecurity, across cloud providers becomes mission critical and can only be achieved through automation and native integration.²

In addition, selecting only one cloud provider drastically impairs competition in the future, effectively leaving DOD captive to one provider. The costs to migrate data or reformat applications from one system to another are likely to be high, deterring the Department from deviating from the incumbent, even if that incumbent’s future technology is clearly inferior to commercial alternatives, when the contract comes up for rebidding at any point in the future.

ITAPS also wants to ensure that the CESG assesses the Total Cost of Ownership (TCO) of the offerings submitted in the coming Request for Proposal (RFP) stage. Individual offerings will vary significantly in the follow-on expenditures required of the Department for testing, maintenance, operations, and security. The optimum balance of security, mission, performance, and TCO can only be achieved by selectively placing applications and mission systems in the appropriate cloud architecture – whether on premises or off premises.

The purpose of the cloud is to relieve enterprises of these burdens, not enhance them – especially when the enterprises have sensitive and critical missions to perform. Mature commercial enterprises intentionally utilize multiple cloud offerings to optimize their computing based on the specific features and pricing of particular cloud stacks. Though we applaud the effort to provide direct guidance to accelerate cloud adoption across the Defense and national security enterprise, we strongly recommend that you consider the following factors as you develop an acquisition strategy:

- Interoperability with mission partners including the Veteran’s Administration, NATO, and the Five Eyes;
- Legacy business and mission systems requirements to migrate to the cloud as some legacy systems need substantive modifications to become cloud ready;
- Total Cost of Ownership that includes data manipulation and access as well as system/data recovery at the end of the Period of Performance; and
- How to avoid a cloud vendor lock-in that limits the swift adoption of new technology to manage data in the future

Policy and Regulatory Barriers

It is becoming increasingly clear that adoption of cloud is not the only challenge the Department faces. One of the largest impediments to achieving cloud adoption is the accreditation/authorization and budgeting process, and, in some cases, hesitancy from some to provide direction along with policy and regulatory barriers. For example, the need to pay for cloud all in one year instead of an elastic model makes budgeting and the demonstration of savings difficult. In addition, the DFARS Network Penetration and Contracting for Cloud Services final rule (Network Penetration rule) has caused confusion with cloud providers. Many of the requirements overlap between Network Penetration rule and the DOD Cloud Security Requirements Guide (SRGs) and there are points of misalignment. The DFARS calls for CSPs to provide adequate security consistent

² Tech Industry’s Recommendations for Federal IT Modernization, August 2017
with FedRAMP Moderate, but within the DOD Cloud SRG, the Level 4 and Level 5 security requirements extend beyond FedRAMP Moderate. Physical separation is no longer seen as a vital requirement for security and in some cases, leaves you less secure. Also, the CAP/IAP is a serious impediment to cloud adoption and is an antiquated model for perimeter defenses and causes a bottleneck for cloud based applications. Additionally, the cyber incident reporting requirements largely appear to overlap, but there is greater context within the DOD Cloud SRG, and it is unclear whether that context also applies to the Network Penetration rule requirements. The Department needs to address points of misalignment and/or formally accept that entities certified under the DOD Cloud SRG meet or exceed the Network Penetration rule requirements via the ongoing reporting obligations under DOD SRG certifications before moving forward on any cloud solution.

Cloud providers have many unanswered implementation questions about this rule which could inhibit cloud adoption and companies from wanting to provide their services to DOD. For instance, must the requirements in DFARS 252.239-7010 flow down to commercial CSPs? DOD can accomplish the intent of the clause by requiring that any prime contractor or managed services provider operating an IT service or system in the cloud on behalf of the government comply with the provisions of the clause. The CSPs have independent obligations arising from their SRG authorizations (required by the clause) that are not aligned directly with the requirements set forth in this clause, and the clause does not reflect the responsibilities assumed by users of the cloud infrastructure as a service (IaaS) (i.e., prime contractors and managed services providers) and the CSPs. For example:

- **DFARS 252.239-7010(b)(2)** requires that the contractor implement controls consistent with the SRG. CSPs will provide SRG-authorized services, but they have no control over what services (be they SRG-authorized or not) that the user of their IaaS uses and no visibility into the impact level of the data that the user is processing in their IaaS. It is the responsibility of the prime contractor/managed services provider to select the services that have received an SRG authorization appropriate to the impact level of the government data. Thus, the prime contractor/managed services provider maintains responsibility for complying with this requirement and it should not flow to the commercial CSP.

- **DFARS 252.239-7010(b)(3)** requires that the contractor maintain all government data “within the United States or outlying areas.” CSPs will provide cloud regions “within the United States or outlying areas,” but they do not select regions for their customers or move customer data among regions. Thus, the prime contractor/managed services provider maintains responsibility for complying with this requirement and it should not flow to the commercial CSP.

- **DFARS 252.239-7010(e)** requires the contractor to submit malicious software to the government. The prime contractor/managed services provider using the IaaS are responsible for responding to malicious software in their cloud environments and submitting that software to DC3. CSPs have independent and defined obligations relating to malicious software in their SRG authorizations.

- **DFARS 252.239-7010(f)** requires contractors to preserve and protect images relating to cyber incidents. The prime contractor/managed services provider using the IaaS has the ability to generate forensically sound snapshots of instances, logs, and any associated network traffic to collect for retention and submission to the DOD.

Additionally, reducing the friction associated with cloud application and data onboarding is critical, and is unfortunately often overlooked in current cloud acquisitions which are too narrowly focused on access to CSP
offerings with no mechanism to support common migration support activities. While the DOD Cloud RFI does ask for information related to cloud migration support services, we recommend expanding this to include all services and offerings that respondents and their partners are able to utilize to reduce onboarding friction from any source—whether it’s from cybersecurity and compliance/regulatory concerns, assistance with application re-factoring, re-architecting, or re-platforming to take advantage of cloud-native services; support strategy, architecture, and design of the target cloud environment, inclusive of desired changes such as a move to dev/ops and continuous delivery and integration modes of operation, or support for organizational elements affected by cloud adoption including cultural adjustments, updated operational models and processes, change management, as well as communication & training plan development.

Another challenge is that though the FedRAMP process is based on the same NIST controls, and DOD is an executive agent in the FedRAMP process, the FedRAMP process and cloud SRG process are different and require different submission packages that unnecessarily increase cost. Further, neither security program provides clear guidance on how to accelerate new technologies into the environment so that the Federal Government or DOD can rapidly take advantage of those technologies. DOD has been very slow to provide guidance as to how they will certify new technologies within the cloud. They continue to apply legacy security and certification toolsets to the cloud environments that they were not designed to integrate with.

The Department should define a cloud security standard that allows the Department to leverage commercially available cloud services in support of its mission objections. The standard should also allow federal contractors to utilize these cloud services in support of their federal contracts, especially where that use is for purposes unrelated to contract performance. DOD should also clarify that cloud services supporting contractor business system management and internal oversight are not subject to the regulations. DOD needs to address many remaining questions on this rule to help accelerate cloud adoption.

Thank you for considering our submission. We look forward to working with the Cloud Executive Steering Group to help accelerate cloud adoption at DOD. If you have any questions, please contact Pamela Walker at pwalker@itic.org or (202)626-5725.

Respectfully,

A.R. “Trey” Hodgkins, III, CAE
Senior Vice President, Public Sector
IT Alliance for Public Sector

CC:  The Honorable Patrick Shanahan, Deputy Secretary of Defense
     Dr. Will Roper, Director, Strategic Capabilities Office (SCO)
Mr. Raj Shah, Managing Partner, Defense Innovation Unit Experimental (DIUx)
Mr. Chris Lynch, Director, Defense Digital Service (DDS)
Mr. Joshua Marcuse, Executive Director, Defense Innovation Board (DIB)
Mr. John Bergin, Business Technology Officer, DOD Chief Information Officer (OCIO)
Mr. Shay Assad, Director, Office of Defense Pricing, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics