904 Clifton Drive, Alexandria, VA 22308
(703) 768-0400 (v) (703) 765-9295 (f)
John@IT-AAC.org www.IT-AAC.org

IT Acquisition Advisory Council (IT-AAC)

Recommendations for Embracing Commercial Cloud in DOD

Mr. Chris Lynch
Director, Defense Digital Service
The White House, USDS
1600 Pennsylvania Ave
Washington DC 20500

The Honorable Ellen Lord
Under Secretary of Defense
Acquisition, Technology, and Logistics (USD AT&L)
3010 Defense Pentagon
Washington DC 20301-3010

Subject: Accelerating Enterprise Cloud Adoption/DoD Cloud RFI

November 17, 2017

Dear Mr. Lynch, Honorable Lord,

We at the IT Acquisition Advisory Council (IT-AAC) have engaged with members of your Cloud Executive Steering Group (CESG), reviewed your RFI and are pleased to provide our coordinated response on your efforts to accelerate DOD's adoption of commercial Cloud solutions to improve DoD mission agility and lower operational costs. As the nation's leading "do tank" on Federal IT Reform, we applaud this effort to usher in commercial Cloud innovations and thereby reduce the risk and cost associated with prolonged reliance on legacy IT infrastructure that is highly brittle and represents a major national security threat if not rapidly modernized.

The IT-AAC, a federation of two dozen leading IT industry groups (NGO) and Standards Bodies (SDO), was chartered in late 2007 to provide Government leaders from Congress, White House and the Executive Branch alternative sources of expertise and insights that are more representative of the $4T Global IT market, of which Federal IT sector is less than 2%. We believe this consolidated response will provide the CESG with an evidenced based approach that can better inform DoD decision makers how to best modernize and secure legacy IT systems that are consuming some 85% of all resources and represent our greatest cyber vulnerabilities.

Our esteemed colleagues and standards partners have reviewed your Cloud RFI as well as related Policies, Laws and significant body of knowledge collected over the past decade. Our approach is rather unique, as the IT-AAC partnership has already hosted over 60 Leadership Working Group sessions on Cloud and related IT modernization issues over the past decade, and believe our synthesis of these findings, informed by the work of leading Cloud standards bodies, should be considered as you seek to migrate legacy IT systems to the cloud. To be consistent with our previous responses to similar requests from Congress, White House and Pentagon IT Reform effort, we would like to share *root cause findings* from our decade long effort to drive sustainable Federal IT reforms before responding to your specific questions;

1. **Removing Barriers to Cloud Innovation:** The goal of adoption of commercial Cloud capabilities is greatly appreciated, and a challenge recognized during the drafting of the Clinger Cohen Act and FITARA. Unfortunately, most of government relies on an antiquated IT acquisition and management process and FFRDC/DIB resources that are "make biased" and drive costly and proprietary IT infrastructure that is program specific. Your vision of embracing Commercial Cloud is timely, and should drive an alternative set of IT management and acquisition processes tuned for the IT market. IT-AAC partners; Cloud Standards Customer Council, Cloud Security Alliance, ICH and TBM Council have several frameworks already proven out and ready for adoption. Currently, DoD has an average of 81 month delivery cycle, and a horrific success rate of only 16% for all major IT programs. IT-AAC has sourced, piloted and standardized a robust Agile Acquisition Framework that has been fully vetted by both govt and industry. As several agencies have already invested in commercial cloud technologies pursuant to the 2011 NDAA Cloud directive, we encourage you to maximize existing investments and lessons learned before embarking on a new path. Given DoD's unique tactical mission, you should find greater value in Hybrid Cloud offerings that are more secure, more scalable, and deployable for our unique war fighter needs.

2. **Workforce and Culture Challenges:** Another challenge that will need to be addressed are gaps in the Defense IT workforce and risk adverse acquisition culture. Defense Acquisition University (DAU) and National Defense University (NDU) will need retool its IT related training and mentoring programs to address unique challenges of sourcing Cloud and other As A Services offerings, that also encourage a greater focus on measurable outcomes, and time to market. New incentives are needed that reward risk tasking and encourage embrace of the 80% solution that is commercially available. This will also require imposing greater restrictions on FFRDCs and UARC are currently competing with the commercial market and perpetuating the status quo.

904 Clifton Drive, Alexandria, VA 22308
(703) 768-0400 (v) (703) 765-9295 (f)
John@IT-AAC.org www.IT-AAC.org

3. **Commercial Standards of Practice**: The CESG clearly understands that the $4T Global IT market is driving Cloud, Network, Mobility standards and innovations. As such, public/private partnerships like the IT-AAC are needed to tap the rich sources of knowledge, expertise and lessons learned. Continued reliance on DoD specific processes like JCIDS, DODAF, FEDRAMP, RMF, are not fully leveraging the work of the International Standards and Commercial IT community of practice who are driving this market. We hope you also consider the significant investment already made by the IT-AAC's partners, including mature Agile Acquisition and Service Level Management frameworks proven to match the speed of innovation. These benchmarked standards of practices have recently been vetted by forward thinking agencies, SEI and GSA FAS to improve decision managing and technology management. On Risk Management, the current FedRAMP and ATO processes are too cumbersome, and relies too heavily on green fields testing that fail to consider the significant body of knowledge and testing results emanating from Fortune 1000 companies. The requirement to have an agency sponsor a new Cloud offering to get an ATO creates a significant barrier to innovation and could lead to a near monopoly and duopoly with a dominant leader.

Again, we applaud the commitment to Commercial Cloud Innovations and DOD's commitment to breaking away from traditional weapon systems approach. However, the CESG and the DoD CMO will need to usher in alternative processes and expertise that are not vested in the status quo. IT-AAC has already established this community of interests and welcomes the opportunity to demonstrate the value of our loosely federated Public/Private Partnership.

Please find our responses below to your specific Cloud RFI questions:

I. Lessons Learned

1. For large customers with a worldwide presence, what kind of personnel resources internal to the customer do you recommend be available to facilitate and support workload migrations? What kind of enterprise program office structure and governance oversight would you recommend based on your experience?

IT-AAC Resp: One approach our standards partners have seen, backed-up by Syndicated Research, is establishing a multi-cloud strategy recognizing there are many types of clouds, each suited for different mission threads, managed by a well-informed CIO shop who have full governance over adoption, management and migration. 85% of Fortune 1000 companies employ a multi-cloud strategy, many using a Cloud Broker concept to orchestrate migration and alignment. IT-AAC has met with benchmarked these lessons learned and glad to share details as appropriate. Our decade supporting DoD, IC, and Civil Agency adoption of Cloud have revealed some interesting insights from both the rare successes and many failures;

1) Don't build it, buy Hybrid Cloud and Hyper Converged Infrastructure this is preconfigured and industry tested. We have documented over 60 viable commercial Cloud offerings suited for every possible need; Back Office, Tactical, ISR Cloud, On-Prem, Off Prem, etc. Knowing your business before jumping into technology is key to your success.
2) Most National Security missions are data and resource intensive, and will require specialize, high performance technology that cannot be shared with less critical applications for the obvious reasons.
3) If continue to mis-apply the current DoD requirements (JCIDS), architecture (DODAF), and procurement (DoD5000) models, this will absolutely fail. OTA's are also not the answer as they eliminate competition and sound decision making.
4) As with any critical technology, Open Architectures defined by consensus based standards bodies, are key to vendor lock-in (BTW, Open Source does not equal Open Architectures).
5) Do not "lift and shift" legacy applications not designed for the Cloud without refactoring. There will be zero savings, and likely increased cost and performance problems.

2. What are the main factors that contribute to system migration failure from your experience? How can those risks be mitigated?

IT-AAC Resp: The main factors to migration failure in DoD specifically are highlighted in our opening augments, and related to common patterns in failure across DOD; workforce shortcomings, over reliance on FFRDC and UARC R&D resources bring a "make-biased approach" (ie. RedDisk, DCGS Cloud, Navy NITROS) that has already wasted hundreds of millions. Over the past decade, IT-AAC has sourced a suite of Agile Cloud and Service Level Management frameworks that have been co-developed with the Cloud standards community. The alternative will be continuing the insanity of using the same process over and over again, or no decision making process at all.

Data collected from early adopters of Cloud in Fortune 1000 provide different failure patterns; one size fits all will not work, more are embracing Hybrid Cloud, using private Hyper Converged Infrastructure for mission critical systems. Infrastructure as a Service is the lowest ROI offering, we documented 14 core shared services that would significantly increase savings. Lift and Shift of legacy systems is a waste of time, and only adds costs. You must refactor legacy apps, or replace them with modern, digital program. All S/W development is very risky and costly, and should be avoided. DoD is not a tech producer and should

904 Clifton Drive, Alexandria, VA 22308
(703) 768-0400 (v) (703) 765-9295 (f)
John@IT-AAC.org www.IT-AAC.org

not try to emulate Google, AWS, Oracle, IBM or Microsoft development efforts as DoD lacks expertise, business model, economies of scale, etc.

3. What kind of customer processes or behaviors have you found essential to enable the optimization of using cloud infrastructure?

IT-AAC Resp: Solution and Service Oriented Architecture (vs DoDAF), Service Level Management framework, Value Stream Analysis to align stake holder value, Performance Based Contracting, and standardized Service and Technology Catalog that aligns with the TBM Council framework. DoD is currently measuring the wrong things which is why most IT programs fail. The first "cloud" DoD should embrace is one that meets its most critical operations using Hyper Converged Infrastructure. This would allow maximum repurposing of hundreds of billions in existing hardware and software licenses DoD already owns.

4. What internal support structures and resources would you recommend for an organization that wishes to capitalize on the sharing of data across the cloud in order to support data-driven decision making and big data analysis?

IT-AAC Resp: A common Data Strategy would be the first step, followed by elimination of program specific IT infrastructure. These stove pipes prevent data sharing, as seen within the struggles of various ISR and Health IT programs that must share data. This is largely a governance problem, which IT-AAC addressed in support of a major restructuring of the AF ISR Portfolio. We are happy to share the details if asked.

5. In your experience, what are the key factors to securing information in an enterprise cloud infrastructure? What are the primary risks to mitigate in this environment?

IT-AAC Resp: Good question. Encryption and Two Factor Authentication are critical for achieving the level of security to host national security programs. Next is role based access that blocks insider threats. The Cloud Security Alliance, Cloud Standards Customer Council and Center for Internet Security have deeper insights. Note also that mission critical program cannot afford potential down time from shared resources or loss of data from insider threats.

II. Pricing and Services III. Tactical Edge IV. Existing Cloud Presence

*** As IT-AAC is not offering any cloud service, these sections are NA.**

V. Policy and Regulatory Barriers

1. Please identify any policies or federal regulations that are barriers to success, explain why those policies or regulations are barriers, and propose revisions or an alternative that still achieves the underlying policy or regulatory objective. Specific suggestions with proposed language revisions are preferred rather than more generalized comments.

IT-AAC Resp: First, the CESG needs to clarify roles and responsibilities between Mission Owners, various CIOs and Acquisition Community, and restructure current governance structure that aligns with unmet CCA and FITARA mandates. Various DFARS 252.239-7010 provisions create significant challenges for Cloud providers with regard to their subs and tech partners, which could inhibit cloud adoption and companies from wanting to provide their services to DoD and interfere with the identification of critical vulnerabilities.

Second, FAR Organizational Conflict of Interests rules prohibit the same organization involved in planning/oversight to also benefit from their recommendations by engaging in implementation work. FFRDC have no immunity, and appear to be an issue resulting from the use of same FFRDC resources who already are deeply involved in existing Cloud operations, OSD Oversight and Open Source development. Additional OCI violations may arise from Mitre's significant investment in Free and Open Source S/W that competes with COTS, including design and development of several Open Source Cloud solutions for Army, Navy, AF and DISA. FAR Part35 also prohibits any FFRDC from performing commercial services or development material solutions, which is a key reason many Silicon Valley start ups are disinterested in working with DoD.

Again, we at the IT-AAC applaud this Cloud vision, and welcome the opportunity to bring in the considerable insights, standards of practice and lessons learned available thru the IT-AAC's elastic public/private "do tank". If you are interested in leverage the considerable investments already made by our esteemed colleagues and public service partners, please take a moment and review these hard hitting reports;

- 2009 Roadmap for Sustainable IT Reform Vol1; http://www.it-aac.org/images/ITAACRoadmapCongSumv1.pdf

904 Clifton Drive, Alexandria, VA 22308
(703) 768-0400 (v) (703) 765-9295 (f)
John@IT-AAC.org www.IT-AAC.org

- 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
- 2017 White House IT Modernization Plan for EO 13800; http://it-cisq.org/wp-content/uploads/2017/10/IT-AAC-Federal-IT-Modernization-Rpt-Signed-9-20-17B.pdf

The Council greatly appreciates the work and dedication of the CESG for its openness to industry input and its transparent efforts to usher in commercial cloud technologies that will offering greater security and mission agility to the war fighter. We stand ready to support the CESG to help usher in emerging standards of practice and lessons learned eliminating from the $4T Global IT market to ensure that the future DoD Cloud adoption achieves both savings and mission agility goals. If you have any question, please contact John Weiler at 703-768-4975 or by email john@IT-AAC.org

Very Respectfully,

John A. Weiler
IT-AAC Exec. Director

Tony Scott
Former Federal CIO

Kevin Green, VADM (ret)
Former Deputy CNO

MGEN Dale Meyerrose, PhD
Former DNI CIO

Honorable John G. Grimes
Former DoD CIO

Dr. Marv Langston
Former Navy & DoD CIO

CC: The Honorable Patrick Shanahan, Deputy Secretary
Dr. Will Roper, Director of the Strategic Capabilities Office (SCO)
Mr. Raj Shah, Managing Partner of the Defense Innovation Unit Experimental (DIUx)
Mr. Joshua Marcuse, Executive Director, Defense Innovation Board (DIB)
Mr. John Bergin, Business Technology Officer, DoD Chief Information Officer (OCIO)