PSC PROFESSIONAL SERVICES COUNCIL
The Voice of the
Government Services Industry

November 17, 2017

The Honorable Patrick Shanahan
Deputy Secretary of Defense
U.S. Department of Defense

Dear Mr. Shanahan:

On behalf of our more than 400 member companies, the Professional Services Council (PSC) respectfully submits this response to the Department of Defense Cloud: Request for Information (Solicitation No. DOD_Cloud_RFI) and your September 13 memo on accelerating cloud adoption.

PSC is the voice of the government technology and professional services industry. PSC's member companies represent small, medium, and large businesses that provide federal agencies and the military with services of all kinds, including information technology (IT) and cloud computing services. As a trade association, PSC focuses its RFI response comments on policy and regulatory barriers that hinder enterprise cloud adoption.

PSC strongly supports Secretary Mattis' goals of accelerating the adoption of innovative technologies and leveraging commercial capabilities to improve our military's warfighting capabilities while saving personnel resources and funding that could be redirected to our warfighters. DOD today has a tremendous opportunity to access innovation and the best ideas that the private sector has to offer. However, the government faces procurement policy and regulatory barriers to acquiring commercial cloud-based or "as-a-service" offerings. PSC appreciates the opportunity to offer policy recommendations to enable DoD to acquire these commercial capabilities.

Should you have any questions, please feel free to contact me at chvotkin@pscouncil.org or Kevin Cummins, PSC Vice President Technology, at cummins@pscouncil.org. Thank you for your consideration.

Sincerely,

Alan Chvotkin
Executive Vice President & Counsel

cc: Hon. Ellen Lord, Under Secretary of Defense, Acquisition, Technology, and Logistics (USD AT&L)

encl.: PSC Response to DOD Cloud: Request for Information

PSC PROFESSIONAL SERVICES COUNCIL

PSC Response to
Department of Defense Cloud: Request for Information

On behalf of our more than 400 member companies, the Professional Services Council (PSC) respectfully submits this response to the Department of Defense Cloud: Request for Information (Solicitation No. DOD_Cloud_RFI) and your September 13 memo on accelerating cloud adoption.

PSC is the voice of the government technology and professional services industry. PSC's member companies represent small, medium, and large businesses that provide federal agencies and the military with services of all kinds, including information technology (IT) and cloud computing services. As a trade association, PSC focuses its RFI response comments on policy and regulatory barriers that hinder enterprise cloud adoption.

PSC strongly supports Secretary Mattis' goals of accelerating the adoption of innovative technologies and leveraging commercial capabilities to improve our military's warfighting capabilities while saving personnel resources and funding that could be redirected to our warfighters. DOD today has a tremendous opportunity to access innovation and the best ideas that the private sector has to offer. However, the government faces procurement policy and regulatory barriers to acquiring commercial cloud-based or "as-a-service" offerings. PSC appreciates the opportunity to offer policy recommendations to enable DoD to acquire these commercial capabilities.

Many of the best practices and lessons learned described below are discussed in more detail in PSC's Tech Corridors Innovation Paper entitled "Delivering Results: A Framework for Federal Government Technology Access & Acquisition" (available at www.pscouncil.org/Downloads/documents/Tech%20Corridors%20White%20Paper%20-%20Final%20-%2012-9-15.pdf) and "Best Practices for Federal Agency Adoption of Commercial Cloud Solutions" report (available at www.pscouncil.org/Downloads/documents/PSC-Cloud-WEB%20-%2012-10-15.pdf).

We thank you for your consideration of the following comments and recommendations.

List of PSC Recommendations

I. Lessons Learned

A. Use existing flexibilities in the Federal Acquisition Regulations (FAR) to accelerate IT modernization.
B. Define requirements in terms of results and outcomes, not technical mandates.
C. Foster competition in the IT marketplace.
D. Do not arbitrarily limit the number of contract awards.
E. Make an early risk assessment.
F. Avoid vendor lock-in.
G. Extend market research beyond this RFI's scope to other as-a-service, cybersecurity, and network on-demand offerings.
H. Consider recommendations from more than just CSPs.
I. Consider procuring services without necessarily buying IT.
J. Leverage existing contract vehicles and capabilities to facilitate IT modernization.

V. Policy and Regulatory Barriers

A. DoD should work with Office and Management and Budget (OMB) and Congress to adapt fiscal law to accelerate IT modernization.
B. Leverage existing budget flexibilities to accelerate IT modernization.
C. Consider a more agile security requirements framework for cloud-based solutions.
D. Amend DoDI 5000.74 – Defense Acquisition of Services to allow reciprocity for cloud security authorizations.
E. Amend DoD Cloud Computing Security Requirements Guide (SRG) to allow reciprocal use of security authorizations and greater use of off-premises cloud solutions.
G. Reassess the Cloud Access Point (CAP) and the Internet Access Point (IAP)programs for network boundary security.

I. Lessons Learned

A. Use existing flexibilities in the Federal Acquisition Regulations (FAR) to accelerate the adoption of new technologies.

To accelerate the adoption of new technologies and move at a speed relevant to the warfighter, DoD should use flexibilities in the FAR to acquire commercial solutions as outcome-based managed services contracts. There is a continuing bias toward government-unique hosting and security requirements that can increase cost and limit access to innovation from the commercial marketplace.

B. Define requirements in terms of results and outcomes, not technical mandates.

Defining contract requirements in terms of results and outcomes is especially important when buying cloud-based technologies compared to purchasing a physical product. Bridging the disconnect that can exist between program officers and contracting officers can help agencies meet this challenge. Technology companies seek to continuously innovate and regularly offer new cloud-based solutions to customers. Mandating DoD-unique technical requirements hinders companies' ability to offer commercial ready innovative solutions, which reduces DoD's ability to leverage private sector investment in commercial offerings. This includes requirements that mandate special protocol analysis or cybersecurity layers that increase latency within the cloud platform. Mission requirements do at times necessitate special requirements such as extra security layers. However, the addition of these requirements may increase latency within the cloud platform and will raise costs and limit competition. The DoD should request these adjustments on an exception-basis only after completing a risk/cost/capability tradeoff analysis. The DoD Secure Cloud Computing Architecture (available at http://www.disa.mil/~/media/Files/DISA/Fact-Sheets/Secure-Cloud-Computing.pdf), which is intended to define a set of logical requirements for cloud security services, is a step in the right direction.

C. Foster competition.

DoD should foster competition for future contract awards. Setting any vendor, product or model/version-specific requirements would exclude potential bidders and reduce DoD's access to commercial market innovation. Companies should be allowed to determine how they can meet the contract requirements and bring their best offer to the table.

D. Do not arbitrarily limit the number of contract awards.

This RFI indicates that a single contract award will be made in 2018. DoD should not set an arbitrary limit to the number of contract awards. DoD is heterogeneous and comprises organizations that vary greatly in terms of size and specific mission needs. DoD should at least consider a multi cloud contract should RFP responses indicate an advantage to doing so. Even if DoD makes an indefinite delivery/indefinite quantity (ID/IQ) contract award to just one commercial cloud vendor, there appears to be additional opportunity for multiple award contracts for consulting, migration services, training, and related services. DISA, as the lead IT

combat support agency, must be directly involved in the acquisition strategy for specific contract requirements.

E. Make an early risk assessment.
Cloud procurement for highly variable and highly uncertain scenarios around military deployment OCONUS creates many challenges compared to buying cloud services for domestic use. DoD should carefully evaluate the risk factors associated with over aggregating cloud capabilities with a single provider, which excludes many potential participants. Conversely, under aggregating capabilities could increase inter-operability challenges and the DoD's ability to leverage new innovation to address unknown future battlefield requirements. In some cases, a cloud-based solution may not be the most appropriate choice for certain workloads or mission requirements.

F. Avoid vendor lock-in.
Competition in the commercial marketplace is driving rapid innovation by technology companies. DoD should position itself to take advantage of this innovation by not limiting itself to the offerings of only one vendor. DoD should acquire cloud services and deploy cloud capabilities where necessary, such that DoD organizations have the ability to migrate their services and capabilities to another CSP later. Otherwise DoD could face challenges of vendor lock-in that limit future innovation and increase costs. Recent advances such as cloud containers also enhance interoperability among CSPs.

G. Expand the scope of RFP to other as-a-service, cybersecurity, and network on-demand offerings.
DoD should strive to adopt the richest form of cloud services. The National Institute of Standards and Technology (NIST) describes three cloud service models: infrastructure as-a-service (IaaS), platform as-a-service (PaaS), and software as-a-service (SaaS). DoD should extend its market research beyond this RFI's scope of IaaS and PaaS to other as-a-service, cybersecurity, and network on-demand offerings. This would allow DoD to potentially harness benefits from bundling cloud services, leverage cybersecurity solutions to provide more flexibility such as tailored services to secure individual workloads within the cloud environment, and enable balanced on-demand solutions encompassing both the cloud service and network connectivity. Software is increasingly delivered as-a-service (SaaS) via the cloud rather than as a product. This shift to SaaS greatly reduces the need to physically own and maintain IT resources. DoD can gain more benefits from cloud when it adopts the richest cloud service possible.

H. Consider recommendations from more than just CSPs.
Cloud technologies are often acquired as part of broader solutions, or in conjunction with additional services that CSPs do not provide, such as deployment, configuration and integration services. Given the barriers between DoD's legacy IT systems and modern cloud-based services, systems integrators and others can provide substantial support services that reduce the risk and time associated with a cloud migration. DoD should consider recommendations from more than just CSPs as part of this RFI process.

I. Consider procuring services without necessarily buying IT.
PSC also recommends that DoD consider procuring services without necessarily buying any IT. A recent example of such an approach is DoD's initiative to replace the Defense Travel System—a complex and expensive customer IT system—with travel services from a commercial travel agency. This approach can be an especially powerful way for DoD to leverage private sector innovation and investment that has already built a solution (such as travel services) for the commercial marketplace in cases where DoD does not have unique requirements.

J. Leverage existing contract vehicles and capabilities to facilitate IT modernization.
Many DoD organizations have existing contracts, and access to governmentwide contract vehicles, to provide cloud brokerage, migration, and provisioning capabilities. These existing contract vehicles should be leveraged for cloud adoption and IT modernization before any acquisition strategy is adopted requiring new contracts for existing capabilities. In addition, many cloud programs could benefit from development prototypes allowed under DoD's existing OTA authority. Rapid procurement under OTA can accelerate successful cloud programs and also identify challenged cloud programs early. OTA could also enable innovative extensions and variations to cloud, including those that must meet the occasional unique requirements of a particular DoD IT program.

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….

A. DoD should work with Office and Management and Budget (OMB) and Congress to adapt fiscal law to accelerate cloud adoption and IT modernization.
The current way that agencies conduct budget planning and Congress appropriates funding creates challenges for cloud adoption. The federal budget process is conducted on an annual basis, and appropriations law generally prohibits an agency from making a future year fiscal commitment beyond what Congress has already funded. Federal procurement rules make it easier for agencies to purchase a physical product, which is purchased in a single fiscal year, compared to as-a-service technologies. Agencies generally buy cloud services using "one year" money from operations and maintenance (O&M) funding. In contrast, the commercial technology marketplace increasingly uses consumption-based purchasing, which private organizations can more effectively leverage than government to take advantage of the flexibility and scalability of cloud computing. This allows organizations to fund IT investments with operational expenditures (OpEx) instead of capital expenditures (CapEx).

While flexibilities do exist in current federal acquisition rules, the legal framework for how government buys technology must adapt to the fundamental shift in the commercial marketplace to consumption-based buying. This "pay as you go" model for buying cloud services can create tremendous problems for DoD organizations at the end of the fiscal year.

For example, a usage spike in September, perhaps as a result of a military surge, would drive up cloud costs during that time. This could place an ongoing (OpEx) program over budget, which today would require DoD to shut it down.

Another model to increasing DoD organizations' access to IaaS, PaaS and SaaS technologies is to use an "evergreen" IDIQ-type contract with specific contract line items (CLINS) for each type of service and a provision allowing vendors to add new services. The government would then issue orders for specific services. Yet this would be administratively burdensome and not very flexible. Similarly, DoD organizations today often develop multiple CLINS so that contracting offices can turn on and off cloud services as needed each month. DoD should seek relief with CLINS that can allow usage flexibility over time.

PSC understands that DoD is already aware of these frustrations. PSC welcomes the opportunity to further engage with policymakers to seek ways to increase contracting and budgeting flexibilities that support the transition to cloud-based and as-a-service technologies. Additionally, contracting officers should be trained on the utilization of and contracting for consumption base contracts to increase cloud adoption.

B. Leverage existing budget flexibilities to accelerate IT modernization.
DoD should leverage existing budget flexibilities to accelerate IT modernization. In addition to using a more flexible approach to buying cloud solutions with O&M funds, DoD could take greater advantage of working capital funds (WCFs) for consumption-based buying of IT services. The appropriate use of WCFs can help agencies take better advantage of the flexibility and scalability of cloud computing. While cloud platforms easily accommodate variable use and surges in demand, this advantage of being in the cloud complicates agency budget planning and contracting. The Air Force addresses a similar challenge created by variable use and spikes in demand for jet fuel by using a WCF to support "into-plane" refueling contracts at foreign airports. Congressional approval of the Modernizing Government Technology Act, which permits federal agencies to establish WCFs that allow investments in IT modernization over a three-year period, may reflect increasing acceptance of the use of WCFs to improve how agencies buy modern technology solutions.

C. Consider a more agile security requirements framework for cloud-based solutions.
Cloud security requirement frameworks impede the ability of DoD to move at the speed of relevancy for the warfighter. DoD policies also prohibit or discourage reciprocal use of security certifications from other DoD and federal organizations such as the FedRAMP Joint Authorization Board (JAB). DoD should expand reciprocal treatment and consider other, more agile methods of authorization such as an initial certification and assessment that is augmented with active monitoring. DoD should apply FedRAMP certification and similar credential requirements to the provider who is delivering the cloud service under a contract, and not necessarily the prime contractor. DoD should encourage companies to propose cloud solutions even if a final contract award is contingent on having a DoD security authorization.

D. Amend DoDI 5000.74 – Defense Acquisition of Services to allow reciprocity for cloud security authorizations.

DoDI 5000.74 – Defense Acquisition of Services impedes access to commercial cloud services and innovation by requiring DoD-specific security authorization before a contract award. Enclosure 7 "Acquisition Considerations for IT within Services (Including IT As-a-Service)" requires that all commercially-provided cloud services have a DoD Provisional Authorization (PA) granted by DISA prior to contract award and an Authority to Operate (ATO) granted by the PM/FSM's Authorizing Official prior to operational use. DoD policy should instead encourage the reciprocal use of FedRAMP JAB authorizations and ATOs issued by other agencies, including other DoD organizations.

E. Amend DoD Cloud Computing Security Requirements Guide (SRG) to allow reciprocal use of security authorizations and greater use of off-premises cloud solutions.

The DoD Cloud Computing Security Requirements Guide (SRG) should require the reciprocal use of, and reliance on, ATOs and PAs from DoD organizations and the FedRAMP JAB. Section 4.5 of the SRG requires a company to obtain a DISA PA before it can respond to a DoD cloud services RFP for an off-premise cloud solution but waives this requirement for a private, on-premises cloud solution. This section should also be amended to allow greater use of off-premises cloud solutions.

F. Reassess the Cloud Access Point (CAP) and the Internet Access Point (IAP) programs for network boundary security.

DoD should reassess the Cloud Access Point (CAP) and the Internet Access Point (IAP) programs for maintaining control over government data flows and protecting the boundary between DoD networks and the cloud. Rather than mandating specific mechanisms to meet security needs, the CAP and IAP should instead set performance-based requirements that focus on desired outcomes. The current boundary protection architecture can increase latency, which impedes access to cloud-based services and innovation. CSPs often have security capabilities residing on their cloud platforms that result in security protection equivalent or similar to CAP without using a network boundary approach.

The Trusted Internet Connection used to protect federal civilian networks creates similar challenges for delivering cloud-based solutions to the government. Significantly, the White House American Technology Council draft "Report to the President on Federal IT Modernization" (available at https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization.pdf) recognizes that this approach to network security creates challenges for civilian agencies wishing to take advantage of commercial cloud services. Greater standardization and the use of performance-based requirements for protecting civilian and military networks could allow for more streamlined CSP accreditation and improve technology companies' ability to offer innovative solutions across the federal government.