PSC PROFESSIONAL SERVICES COUNCIL
The Voice of the
Government Services Industry

March 21, 2018

The Honorable Patrick Shanahan
Deputy Secretary of Defense
1010 Defense Pentagon
Washington, DC 20301-1010

Dear Mr. Shanahan:

The Professional Services Council (PSC) respectfully requests that the Cloud Executive Steering Group (CESG) expand the scope of its current efforts to accelerate cloud computing adoption to include removing policy and regulatory barriers to leveraging cloud-based technologies across the Department of Defense (DoD).

PSC's 400 member companies represent small, medium, and large businesses that provide civilian agencies and the military with services of all kinds, including information technology (IT) and cloud computing services. PSC supports Secretary Mattis' goals of accelerating the adoption of innovative technologies and leveraging commercial capabilities to improve our military's warfighting capabilities. PSC further supports DoD's commitment to full and open competition for the upcoming Joint Enterprise Defense Infrastructure (JEDI) Cloud solicitation.

Cloud computing provides a powerful platform to deliver new tools to the warfighter and improve national defense. Yet significant policy and regulatory barriers still stand in the way of adopting cloud-based technologies. These barriers impede DoD's ability to move at the "speed of relevancy" to the warfighter. While DoD sought and received public comment on policies and regulations that are barriers to the success of the JEDI Cloud initiative, the subsequent draft solicitation and industry day presentations do not address these obstacles.

Flexibilities do exist in current federal acquisition rules. The legal framework for how DoD and civilian agencies buy technology, however, must still adapt to the fundamental shift in the commercial marketplace to consumption-based buying. Certain cybersecurity requirements can also unduly hinder the ability to deliver innovative commercial capabilities to the warfighter without compromising security. We thus ask that CESG act on the enclosed list of PSC recommendations for removing or modifying policies and regulations to broaden and speed up DoD's cloud adoption.

PSC also welcomes the opportunity to further engage with CESG and your staff, as well as with policymakers across the government, to provide additional details and to offer our support for removing these barriers. Thank you for your consideration.

Sincerely,

Alan Chvotkin
Executive Vice President and Counsel

encl: PSC Recommendations for Removing Policy and Regulatory Barriers to DoD Cloud Adoption

cc: Hon. John Gibson, Chair, Cloud Executive Steering Group and Chief Management Officer, U.S. Department of Defense

Hon. Ellen Lord, Under Secretary of Defense for Acquisition and Sustainment, U.S. Department of Defense

PSC
PROFESSIONAL
SERVICES
COUNCIL

PSC Recommendations for Removing Policy and Regulatory Barriers to DoD Cloud Adoption

List of Recommendations

1. DoD should work with Office of Management and Budget (OMB) and Congress to adapt fiscal law to accelerate cloud adoption.

2. Leverage the funding flexibility provided by the Modernizing Government Technology Act.

3. Consider a more agile security requirements framework for cloud-based solutions.

4. Amend DoDI 5000.74, Defense Acquisition of Services, to allow reciprocity for cloud security authorizations.

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

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

Explanation

1. DoD should work with Office of Management and Budget (OMB) and Congress to adapt fiscal law to accelerate cloud adoption.

The way agencies currently conduct budget planning and how Congress appropriates funding creates challenges for accelerating cloud adoption. The federal budget process is conducted on an annual basis. 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 operation 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. This problem can be exacerbated by the constraints imposed under a Continuing Resolution for funding DoD, which has occurred for the past nine years.

Another model for increasing DoD organizations’ access to as-a-service 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 approach can be administratively burdensome and inflexible. 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 and welcomes the opportunity to further engage with policymakers to seek ways to increase contracting and budgeting flexibilities that support the transition to cloud-based technologies.

2. Leverage the funding flexibility provided by the Modernizing Government Technology Act.
In addition to using a more flexible approach to buying cloud solutions with O&M funds, DoD should leverage existing budget flexibilities including the working capital fund (WCF) mechanism provided by the Modernizing Government Technology (MGT) Act.[1] 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. The MGT Act allows DoD to apply this same principle to cloud computing and other innovative technologies through an IT Working Capital Fund.

3. 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 to the warfighter. DoD policies 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.

[1] *see:* Pub. L. No. 115-91, Title X, Subtitle G. § 1077(b)(1).

4. 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 authorizations 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 the Defense Information Systems Agency (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 amend DoDI 5000.74 to encourage the reciprocal use of FedRAMP JAB authorizations and ATOs issued by other agencies, including other DoD organizations.

5. 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 Request for Proposal (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.

6. 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. Relying on these capabilities could speed performance without sacrificing security.

The Trusted Internet Connection used to protect civilian networks creates similar challenges for delivering cloud-based solutions to the government. Significantly, the White House American Technology Council "Report to the President on Federal IT Modernization" recognizes that this approach has "resulted in security implementations that negatively affect performance and create barriers to use of commercial [cloud] technology."[2] Greater standardization and the use of performance-based requirements for protecting civilian and military networks could allow for more streamlined CSP accreditation and thus improve technology companies' ability to offer innovative solutions across the federal government.

[2] White House. Report to the President on Federal IT Modernization. Dec 13, 2017, p6. *available at*: https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf, *accessed:* Mar 20, 2018.