February 1, 2019

Mr. Joshua Marcuse
Executive Director
Defense Innovation Board
3030 Defense Pentagon
Room 5E572
Washington, DC 20301-3030.

Dear Mr. Marcuse:

The Professional Services Council (PSC) respectfully requests that the Defense Innovation Board (DIB) consider these comments in response to its Software Acquisition and Practices (SWAP) study and working document draft legislative language for a new category or pathway to procure software for DoD applications ("Section 805 Draft Language").[1]

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 software services. PSC supports DIB's mission to catalyze innovation in the Department of Defense (DoD). PSC further supports efforts to accelerate the adoption of innovative technologies to improve our military's warfighting capabilities. In particular, PSC appreciates DIB recommendations encouraging DoD to leverage commercial innovation and contractor-developed and financed applications solutions.

PSC supports greater use of existing flexibilities in current federal acquisition rules, such as the commercial item preference in 10 U.S.C. 2377. Section 805 of the National Defense Authorization Act for Fiscal Year 2016 (NDAA, Pub. L. No. 114–92) directed DoD to establish procedures for alternative acquisition pathways to acquire critical national security capabilities. This legislative mandate further emphasizes that the procedures shall maximize the use of flexibilities in existing law and regulation. However, the legal framework for how DoD buys technology must still adapt to the fundamental shift in the commercial marketplace to consumption-based buying and cloud technologies, such as software as a service (SaaS). Certain cybersecurity requirements can also unduly hinder the ability to deliver innovative commercial capabilities to the warfighter without compromising security.

---

[1] Appendix L.3: Section 805 Template Language for Chapter 4, Option 3. V0.2, 14 Jan 2019. *available at:* https://media.defense.gov/2019/Jan/15/2002080006/-1/-1/0/DIB_SEC805_DRAFT_POSSIBLE_LANGUAGE_2019.01.14.PDF, *accessed:* Jan. 18, 2019.

PSC appreciates DIB's efforts to engage with industry as it develops its recommendations. Many of the draft DIB recommendations touch on complex challenges facing DoD as it seeks to accelerate software development and leverage commercial innovation while also ensuring security and cost-effectiveness. PSC will continue to engage with our members to identify best practices and recommendations for DoD software development and share those with DIB.

At this time, we ask that DIB consider the recommendations below as it finalizes its report to senior defense leaders:

I. PSC Overall Comments on DIB SWAP Study Recommendations

1. Add a new recommendation that DoD solicitations for software and other IT-related acquisitions focus on desired outcomes rather than inputs.
DoD solicitations for software should focus on desired outcomes rather than inputs. The adoption of outcome-based solutions allows government to strategically partner with industry and gain the value of industry best practices, on-going research and development and a sharing of risks and rewards. For example, DoD solicitations could require the use of Statements of Objectives, instead of Statements of Work, and explicitly allow for alternative proposals that will be fully evaluated and scored.

2. Include clear language encouraging DoD to remove policy and regulatory barriers to leveraging software as a service (SaaS) and cloud based-technologies.
Cloud computing provides a powerful platform to harness data and deliver new tools for analysis and decision making that ultimately enhances warfighter lethality and improves national defense. Yet significant DoD policy and regulatory barriers still stand in the way of adopting software as a service (SaaS) and other cloud-based technologies. These barriers impede DoD's ability to move at the "speed of relevancy" to the warfighter.

For example, DoD policies prohibit or discourage reciprocal use of vendors' security certifications from other DoD and federal organizations such as the FedRAMP Joint Authorization Board (JAB). The DoD Cloud Computing Security Requirements Guide (SRG) should require the reciprocal use of, and reliance on, authorizations to operate (ATOs) and provisional authorizations (PAs) from DoD organizations and the FedRAMP JAB. Section 4.5 of the SRG currently requires a company to obtain a DISA provisional authorization before it can respond to a DoD cloud services Request for Proposal (RFP) for an off-premise cloud solution. In addition, DoD should amend DoDI 5000.74, Defense Acquisition of Services, to allow reciprocity for cloud security authorizations and more flexibility for vendors to offer software tools that do not have a DoD-specific security authorization during the contract award phase.

DoD should also consider a more agile security requirement than the Cloud Access Point (CAP) and the Internet Access Point (IAP) programs for protecting the boundary between DoD networks and the cloud. This perimeter-based approach to security can create latency issues that hamper the use of SaaS tools. Rather than mandating specific mechanisms to

meet security needs, the CAP and IAP should instead set performance-based requirements that focus on desired outcomes.

3. DIB should encourage a consistent approach to IP management across the Department, with a preference for limited data delivery.
PSC recommends that DoD seek a consistent approach to IP management across the Department, but with a preference for obtaining limited data delivery. Some non-traditional defense companies cite the IP requirements of standard, Federal Acquisition Regulation (FAR) based contracts as a barrier to working with DoD. The Army recently adopted a new IP policy designed to discourage scenarios where the Army requests too little or too much IP.[2] However, the Army IP policy focuses on new systems, not sustainment. DIB should encourage consistency in IP management policies across military branches and robust communication with industry to avoid confusing and inconsistent terms and requirements in solicitations.

4. Include greater consideration of how DoD can accelerate software development and deployment while meeting the imperative to improve cybersecurity and software supply chain security.
The DIB Working Draft TL;DR document (V1.5 11 Jan 2019) emphasizes that contractors need to adopt DevSecOps practices/culture and prioritize speed as a critical metric. There are benefits to using a framework such as DevSecOps to include security as an integral part of the software life cycle. However, the DIB should also consider how DoD can accelerate software development and leverage commercial solutions at a time of increased concern about defense industrial base resiliency and supply chain security.

II. PSC Comments on specific DIB SWAP Study Recommendations (V0.1, 14 Jan 2019)[3]

DIB Recommendation 5 - Create standardized regulatory and IP language for open source, proprietary, and government-funded code that allows DoD to maintain appropriate control of its code base.
As noted above, this draft recommendation could be strengthened by recommending that DoD seek a consistent approach to IP management for both new systems and sustainment. It is also important that the DoD contracting workforce is educated and trained to comply with new policies effectively.

---

[2] Suits, Devon. "Army secretary approves new Intellectual Property Management Policy." Army News Services. Dec. 11, 2018. *available at:*
https://www.army.mil/article/214881/army_secretary_approves_new_intellectual_property_management_policy *accessed:* Jan. 22, 2019
[3] Working Document Draft, DIB SWAP Study Recommendations "Cheat Sheet," *available at*:
https://media.defense.gov/2019/Jan/15/2002080004/-1/-1/0/DIB_PRELIMINARY_RECOMMENDATIONS_FOR_FEEDBACK_2019.01.14.PDF, *accessed:* January 18, 2019

DIB Recommendation 8 *- require that all systems purpose-built for DoD should have their source code available to the Department. DoD should have the rights to and be able to modify the code when new conditions and features arise.*

PSC opposes this broad recommendation that all systems purpose-built for DoD have their source code available to the Department. This could be cost prohibitive to DoD, discourage some vendors from offering software services to the Department, and create a barrier to accessing the innovation DoD seeks to meet today's national security needs. Some companies already avoid becoming DoD industry partners or seek to do so only with IP flexibilities available under Other Transaction Authority (OTA) but not FAR-based contracting.

DIB recommendation 31 *- Exempt the DoD from the Clinger Cohen Act (to remove unnecessary bottlenecks for the use of modern IT systems for combat systems).*

PSC does not support a wholesale exemption of DoD from the Clinger-Cohen Act (40 U.S.C. 1401 et seq.), which gives the DoD Chief Information Officer (CIO) the responsibility of developing and maintaining an integrated IT architecture as well as identifying major IT acquisition programs that have significantly deviated from their respective cost, performance or schedule goals.

DIB Recommendation 33 *- Allow the use of working capital funds for software development, deployment, and sustainment.*

PSC supports DoD implementing a Working Capital Fund for IT Modernization and cloud technologies. PSC's understanding is that DoD has the authority to do so under both Title 10 (e.g. 10 U.S.C. 2208) and the Modernizing Government Technology Act (Pub. L. No. 115-91, Title X, Subtitle G. § 1077(b)(1)). This recommendation could also be combined with the related recommendation no. 48 (see comments below).

DIB Recommendation 36 *- Waive the requirements of the Antideficiency Act to enable to use of software as a service (SaaS) contracts for DoD systems.*

PSC supports this in concept but urges DIB to make a stronger recommendation that DoD work with the Office of Management and Budget (OMB) and Congress to adapt fiscal law to accelerate the adoption of software as a service (SaaS) and other cloud-based technologies.

The way agencies currently conduct budget planning and how Congress appropriates funding creates challenges for using SaaS tools. 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 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 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 problem can be exacerbated by the constraints imposed under a Continuing Resolution funding DoD.

PSC understands that DIB 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 SaaS and other cloud-based technologies.

DIB Recommendation 37 – *More frequently use "challenge-based acquisition" to promote a competitive environment, demonstrated performance, and an increased partnership with industry.*
PSC supports the appropriate use of "challenge-based acquisition" for software, which allows offerors to demonstrate their capability or solution rather than just describe it in a written proposal. Challenge-based acquisitions can include hosting demonstration days, establishing a series of technical milestones before awarding a contract, or incorporating technical demonstrations or development challenges as part of formal proposal evaluation criteria during the acquisition process. As noted in the draft DIB "Ten Commandments of Software,"[4] software budgets and acquisitions should consider the full life-cycle costs of software when evaluating competitors' proposals. An award based on lowest price following down-selects after the technical challenge process would rarely be the appropriate source selection methodology.

DIB Recommendation 48 - *Pilot and then establish a "Department of Defense Rapid Software Development Fund'' to provide multi-year funds for acquisition programs making use of rapid software development pathways.*
This proposed rapid software development fund could instead be a part of a broader working capital fund (WCF) to support IT modernization and the acquisition of "consumption-based" IT services such as SaaS. Regardless of the specific WCF mechanism, DoD should leverage existing budget flexibilities to support buying SaaS solutions with O&M funds. The appropriate use of WCFs can help agencies take better advantage of the flexibility and scalability of cloud-based technologies. 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

---

[4] *available at:* https://media.defense.gov/2018/Apr/22/2001906836/-1/-1/0/DEFENSEINNOVATIONBOARD_TEN_COMMANDMENTS_OF_SOFTWARE_2018.04.20.PDF; *accessed:* Jan. 31, 2019.

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. DoD also has existing authority to establish WCFs under Title 10 (e.g. 10 U.S.C. 2208).

III. PSC Comments on DIB Draft Section 805 Template Language[5]

Section _____ (d) SOFTWARE FUND

The draft legislative language includes a section establishing a new Software Fund (Sec _____ (d)). This section could instead be drafted to direct DoD to establish a broader WCF for IT acquisition under its existing authority from Title 10 or an IT Working Capital Fund under authority provided by the MGT Act.

See also our comments above on DIB draft recommendations 33 and 48.

IV. Conclusion

PSC welcomes the opportunity to further engage with DIB, as well as with policymakers across the government, to provide additional details and to offer our support for removing barriers to rapid software acquisition and as-a-service technologies. As noted above, PSC appreciates DIB's continued efforts to engage industry early and often in developing and refining its software recommendations.

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

Sincerely,

Alan Chvotkin, Esq.
Executive Vice President and Counsel

---

[5] *available at*: https://media.defense.gov/2019/Jan/15/2002080006/-1/-1/0/DIB_SEC805_DRAFT_POSSIBLE_LANGUAGE_2019.01.14.PDF, *accessed*: Jan. 18, 2019