October 24, 2018

The Honorable Suzette Kent
US Federal Chief Information Officer
Office of Management and Budget
725 17th Street Northwest
Washington, DC 20503

Via email to: ofcio@omb.eop.gov

Re.: Comments on Draft Cloud Smart Strategy

Dear Ms. Kent,

BSA | The Software Alliance[1] appreciates the opportunity to offer comments on the Office of Management and Budget's (OMB) Draft Cloud Smart Strategy (Draft Strategy). We commend the commitment to improving upon the current Cloud First Strategy and increasing cloud adoption across the Federal Government. We specifically welcome the Draft Strategy's focus on security, procurement, and workforce, each of which has an important impact on cloud adoption.

Our members lead the world in offering cutting-edge cloud technologies that can help governments be more responsive to constituents, and more nimble, productive, and innovative, while also improving network security and system availability. We are encouraged by OMB's willingness to take further steps to promote the adoption of cloud solutions and offer the comments below to support this goal.

I - GENERAL CONSIDERATIONS

We encourage OMB to continue consulting with stakeholders as this Draft Strategy is implemented and when other related policies, guidelines, and rules are developed. In

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Akamai, ANSYS, Apple, Autodesk, Bentley Systems, Box, CA Technologies, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, and Workday.

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

addition to public comment opportunities, OMB should encourage the use of workshops and other appropriate mechanisms for convening stakeholders.

Cloud Service Providers (CSPs) are constantly innovating and offering new and improved cloud services. The federal government will be able to leverage the full benefits of cloud computing only if it implements policies that empower agencies to adopt cloud services in a manner that is agile, flexible, and informed by industry expertise.

A non-prescriptive, technologically neutral strategy will help federal agencies keep pace with changes in the cloud computing environment, allowing for the adoption of cloud services that create cost-benefits and efficiency. A flexible strategy is also important to accommodate all types of services that are encompassed by the term "cloud computing." Although some elements of the Draft Strategy – such as actions to develop, hire, and retain a skilled workforce – apply to all types of cloud computing services equally, other elements will vary depending on the type of cloud offering being considered. Security requirements, technical support, and other procurement terms must be tailored to the cloud deployment model under consideration (e.g., Infrastructure as a Service (IaaS) vs. Platform as a Service (PaaS) vs. Software as a Service (SaaS)). For instance, a CSP offering an IaaS solution will manage underlying infrastructure, and the agency will be responsible for operating systems, middleware, and applications – this allocation of responsibilities must be considered in all phases of the agency cloud strategy including planning, procurement, and management of the services. A different set of considerations must be taken into account when the solution sought is a PaaS or SaaS.

Finally, the Draft Strategy should make it very clear that the adoption of cloud services should be based on a search that is technology-neutral, platform-neutral, and deployment model-neutral.

Recommendations:

- We recommend private sector input and best practices be considered as the Draft Strategy is implemented and further updated.
- The Draft Strategy should be flexible to allow federal agencies to keep pace with cloud computing innovations and enable agencies to consider the type of cloud computing offerings (IaaS, PaaS, or SaaS) that they require to meet their needs.
- We urge the Draft Strategy highlight that the solution selection should always focus on the agencies' objectives and be neutral regarding the technology, platform, and service model to be adopted.

II - SECURITY

Security Measures Based on Risk and Industry Best Practices

We welcome the Draft Strategy's recognition that security is key to successfully implementing cloud solutions. We particularly support the risk-based approach to security taken by the Draft Strategy. Security requirements should prioritize outcomes rather than prescriptive mechanisms to achieve those outcomes. The perpetrators of cyber-attacks are constantly adjusting their methods, targets, and technologies. The imposition of highly prescriptive security rules must be avoided as they fail to recognize new and evolving methods and technologies which could, in turn, limit the ability of CSPs and others to anticipate and respond to emerging threats.

Security measures should be based on risk management and should vary depending on the sensitivity level of the data. This approach prevents unnecessarily burdensome rules, while allowing more robust security measures are applied where needed. The data classification criteria should also be revisited from time to time to ensure that changes in the sensitivity of the data are reflected on the level of security required to protect them.

Furthermore, security measures should focus on application and data-level security, including using of robust encryption. This will enable federal agencies to acquire solutions that are both more secure and better suited to their specific missions. Strong encryption is a fundamental building block to any robust approach to data security. As the government moves forward with the implementation of the Draft Strategy, federal agencies should be encouraged to implement encryption solutions that enhance security with minimal burden on the user.

We also agree with the Draft Strategy's assessment that the use of a limited number of Trusted Internet Connections (TIC) to secure all agency network traffic flow is no longer feasible as a one-size-fits all solution. It is necessary to go beyond reliance on either legacy TIC or DHS's Continuous Diagnostic and Mitigation (CDM) program approach. The focus should be on security outcomes rather than technology mandates.

The Federal Risk and Authorization Management Program (FedRAMP)

OMB requires federal agencies to use FedRAMP to ensure the cloud services they procure are secure. BSA agrees that FedRAMP should continue to serve as a security benchmark. We also agree that that there is a strong need to make improvements to the FedRAMP authorization process.

Greater efficiency in initial authorization to operate could be achieved by enabling agencies to leverage Joint Authorization Board (JAB) Provisional Authority to Operate (ATO) without a re-review process. In addition, continuous monitoring, which imposes significant costs on both cloud providers and agencies (particularly in the JAB context), should be improved to be more responsive to agencies' needs and cloud providers' capabilities.

Recommendations:

- The Draft Strategy should emphasize that a risk-based approach should be taken to increase security in a cost-effective manner.
- The Draft Strategy should caution agencies not to impose all-encompassing security requirements that introduce undue complexity and high costs.
- As federal agencies transition out from the current TIC approach, they should increase their use of monitoring tools that are made available by CSPs.
- The Draft Strategy should stress the need to further explore opportunities to reduce the time and complexity of achieving and maintaining a FedRAMP ATO and to change baseline requirements to enable further use cases.

III - PROCUREMENT

Flexibility and Agility

Government procurement policies have an enormous impact on agencies' ability to adopt cutting-edge cloud services. Traditional purchasing practices and contract terms may hinder the scalable, cost-effective, and innovative nature of cloud computing. The

procurement of cloud offerings does not fit the traditional purchasing model applied to physical IT products and other commodities. Flexible and agile procurement processes that are not hampered by burdensome terms and conditions will allow users to fully leverage the vast array of benefits offered by cloud computing technologies.

Budgeting and resource allocation practices for the procurement of cloud services also need to be reconsidered. Unlike the acquisition of traditional commodities that are considered capital expenses, cloud services are often offered via "on demand" or subscription terms that are more akin to operating expenses. Agencies should be given guidance on how to budget and manage expenses in a way that allows them to analyze and forecast cloud needs to avoid under- or over-budgeting, which could have an impact on the continuity of services or efficient use of taxpayer dollars. A modern acquisition model for cloud services should provide federal agencies with flexibility to procure these services in a manner that accounts for dynamic changes in demand while complying with budgetary requirements.

Use of Vendor-Supported Cloud Solutions

We appreciate that the Draft Strategy directs federal agencies to consider commercial solutions as appropriate. The use of commercially available technologies minimizes implementation times, increases efficiency, and avoids the costs associated with custom technology development.

Commercial solutions also provide significant post-deployment cost and security benefits as such solutions can be more easily updated to address new agency needs as well as potential new vulnerabilities. An increase in agencies' use of commercially available cloud solutions would prevent operations and maintenance costs from consuming a large part of the federal IT budget and would free up resources for IT modernization investments. To protect their investment, it is imperative that federal agencies work with CSPs with a proven track record of offering robust and reliable support for cloud offerings.

Finally, contract terms that are specific to government procurement contracts add unnecessary costs and create inefficiencies. These terms should be avoided to ensure the federal government can fully leverage the benefits of state-of-the-art and cost-effective technology.

Overly Broad Application of Federal Acquisition Regulation (FAR) Rules

Public procurement contracts often include numerous references to FAR provisions regardless of whether they are actually relevant to a particular transaction. Many procurement officers will over-apply FAR terms and will limit providers' ability to negotiate away those terms that are clearly inapplicable.

We recognize that contracting officers should make every effort to comply with FAR. However, over-application of FAR rules that fail to consider the specifics of cloud computing offerings with the sole objective of avoiding litigation risks is not what the regulation seeks to accomplish. Indeed, the FAR directs agencies to adopt acquisition strategies that are predicated on "risk management" rather than "risk avoidance" because "[t]he cost to the taxpayer of attempting to eliminate all risk is prohibitive."[2] Accordingly, FAR directs the Executive Branch to "accept and manage the risk associated with empowering local procurement officials to take independent action based on their professional judgment."

[2] Federal Acquisition Regulation, Section 1.102-2(c)(2).

Recommendations:

- The Draft Strategy should clearly direct procurement officers to follow well-established federal policy and procure commercial cloud offerings whenever possible.
- The Draft Strategy should direct federal agencies to prioritize the selection of cloud solutions for which the CSP (or some other commercial partner) offers reliable support. This should apply equally to all types of cloud services (IaaS, PaaS, and SaaS).
- The Draft Strategy should encourage contracts to be streamlined by eliminating government-specific terms and conditions for commercial cloud offerings.
- The Draft Strategy should urge procurement officers to use their professional judgment to consider whether FAR provisions are actually relevant to a particular contract and that rules should not be added if they are not necessary.

IV - WORKFORCE

Agencies should strive to develop, hire, and retain a workforce with the necessary skills to leverage cloud computing in ways that advance their missions. As the Draft Strategy rightly recognizes, identifying the necessary skills and the existing gaps is an important first step.

Addressing the shortage of workers with cloud computing skills should include actions that target the entire workforce spectrum. Actions should include improving interest in and access to computer science education for K-12 students, with a focus on expanding public-private partnerships, re-envisioning vocational education, and training more STEM-qualified K-12 teachers. (For example, NASA and the NSA regularly invest in K-12 STEM education efforts.)

It also important to focus on mid-career retraining programs to provide American workers with high-demand cloud computing skills. This should include initiatives to allow Federal agency employees to leverage private sector expertise for training on a variety of cloud computing skills and best practices. Many CSPs offer training programs that are free of charge or included as part of procurement contracts.

Agility in hiring qualified professionals is also important. The Office of Personnel Management (OPM) has recently announced direct hire authorities for federal agency job candidates for Cybersecurity and other STEM positions.[3] This initiative is important to and should be fully implemented.

Recommendations:

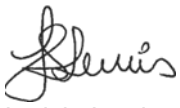
- The Draft Strategy should promote actions to improve STEM, including computer science and education for K-12 students.
- The Draft Strategy should highlight the importance of programs to train mid-career workers both in and outside government. Training should leverage programs offered by industry, particularly by CSPs.

[3] Government-Wide Direct Hire Authorities available at https://www2.usgs.gov/humancapital/sw/FSGovWideDirectHire.html.

- The Draft Strategy should highlight OPM's direct hire authorities for federal agencies to more quickly hire workers with the necessary skills to foster the adoption of cloud computing by federal agencies.

We appreciate the opportunity to share these initial recommendations, and we also look forward to a broader conversation about how the software industry can work with OMB and federal agencies across the federal government to help them generate value from their investments in commercial cloud offerings.

Sincerely,



Leticia Lewis
Director, Policy

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org