September 20, 2017

To: Ms. Margie Graves
Acting Chief Federal Chief Information Officer
Director, CIO Council

Filed via email to: itmodernization@cio.gov

From: BSA | The Software Alliance

Re: Comments on the Report to the President on Federal IT Modernization

---

I. Introduction

BSA | The Software Alliance ("BSA") welcomes this opportunity to offer its comments on the American Technology Council's ("ATC's") Report to the President on Federal IT Modernization (hereinafter the "Report").[1] BSA advocates for the global software industry before governments around the world and in the international marketplace. BSA's member companies include several of the world's leading developers of software and other information technology ("IT") products and services, many of which are IT partners with federal agencies.[2]

BSA welcomes the Report's goals of improving and updating federal IT systems to take advantage of modern commercial technologies and to streamline federal IT procurement and deployment practices. With only a few exceptions noted later in these comments, we believe the Report's recommendations will make federal agencies better able to fulfill their missions and improve government services, advance their cybersecurity posture, and make the operation of government IT systems more cost effective. BSA specifically welcomes the Report's recommendations that federal agencies "leverage American innovations through

---

[1] ATC, *Report to the President on Federal IT Modernization* (2017), *available at* https://itmodernization.cio.gov/.

[2] BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corporation, The MathWorks, Trend Micro and Workday. More information on BSA and its members is available at http://www.bsa.org/about-bsa/bsa-members.

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

increased use of commercial technologies"[3] and that agencies "build[] new capabilities *only* when shared services and commercial technologies cannot meet mission need."[4]

BSA also strongly supports the Report's recommendations to increase federal agencies' use of commercial cloud services and infrastructure and to accelerate their adoption of cloud-based email and collaboration tools.[5] US technology firms lead the world in offering cutting-edge cloud technologies and solutions that can help government agencies be more nimble, productive, and innovative, while also improving network security and system availability. As the Report recognizes, "[m]ajor commercial cloud infrastructure providers offer excellent levels of functionality, cost effectiveness, and security because of their ability to aggregate demand across a broad range of customers."[6] Accordingly, "[r]ather than relying on often outdated and agency-specific systems, the Federal Government could leverage these providers' expertise to both save taxpayer dollars and increase effectiveness and security."[7]

BSA agrees with these conclusions, and our member companies are eager to work with agencies across the Federal Government to help them generate value from their investments in commercial cloud offerings. In this regard, BSA applauds the Report's reference to work being done to reduce the time and complexity of the process of achieving and maintaining a FedRAMP Authority to Operate (ATO). Building on this, ATC should explore opportunities for greater efficiencies in: 1) initial authorization, enabling agencies to leverage Joint Authorization Board (JAB) Provisional ATOs without re-review; and 2) continuous monitoring, which imposes significant costs on both cloud providers and agencies, particularly in the JAB context, and could be evolved to be more responsive to agencies' needs and cloud providers' capabilities. We also thank the Administration for presenting innovative acquisition tactics to empower agencies to purchase shared cloud services,[8] and believe that such initiatives will benefit from the participation, expertise, and insights of the full community of cloud vendors.

As the Report recognizes, achieving more widespread adoption of commercial cloud offerings by federal agencies will necessitate a partial shift in approach to managing the security of federal networks--specifically, away from an approach focused on securing the network perimeter and towards a more layered, defense-in-depth approach.[9] BSA welcomes these recommendations. As federal agencies increasingly consume IT resources as services, including over mobile devices, focusing on application and data-level security, including through the use of robust encryption,[10] rather than relying primarily on hardening the network

---

[3] *Report*, *supra* n. 1, at 2.

[4] *Id.* at 18 (emphasis added).

[5] *See, e.g.*, *id.* at 17-24.

[6] *Id.* at 19.

[7] *Id.* at 18.

[8] *See id.* at 40.

[9] *See, e.g.*, *id.* at 11 (recognizing need to update federal security programs "to enable a layered security architecture that facilitates transition to modern computing in the commercial cloud").

[10] As the Report acknowledges, strong encryption is a fundamental building block to any defense-in-depth approach to cybersecurity. As the government moves forward with implementation of this Report, agencies should be encouraged to implement encryption solutions that enhance security with minimal burden on the user. In addition, the US should continue to invest in research and development of cutting

perimeter, will increase the range of available IT options for agencies and make it easier for them to acquire commercial solutions that are both more secure and better suited to their unique missions. Strong encryption is a fundamental building block to any defense-in-depth approach to cybersecurity. As the government moves forward with implementation of this Report, agencies should be encouraged to implement encryption solutions that enhance security with minimal burden on the user. In addition, the US should continue to invest in research and development of cutting edge encryption technologies and should avoid policy initiatives that would have the effect of chilling such efforts.[11]

In short, we applaud the vast majority of recommendations set forth in the Report and encourage the Administration to act on them. In addition, we offer the following specific comments and suggestions in the hopes that they will provide greater clarity to federal agencies and help advance the objectives set forth in the Report.

II. Specific Comments

A. Risk of Overreliance on Lowest Price, Technically Acceptable Criteria

Particularly as many federal agencies seek to rein in spending, BSA appreciates the need for agencies to achieve the greatest value possible for their IT investments. In light of this goal, BSA is concerned that the Report's lack of specific guidance on how to evaluate the relative value of computing IT solutions may lead some agencies to over-rely on lowest price, technically acceptable ("LPTA") source selection criteria as they seek to modernize their IT systems.

Although LPTA source selection criteria can be appropriate for certain procurements, its use for IT procurements often discourages agencies from selecting products or services that offer greater value to the agency than the lowest-priced option. For IT procurements, that additional value can manifest itself in many different ways--for instance, in the form of better security, additional functionality, superior product support, or greater ease of use. LPTA also may restrict an agency's consideration of past performance as a factor in the procurement process, thus forcing it to ignore information that may, as a practical matter, be highly relevant. Over-reliance on LPTA source selection criteria thus raises a substantial risk that federal agencies may feel compelled to select the "cheapest" IT solution, even if that solution does not provide the lowest overall cost of ownership and does not offer the best value for the government's money.

Concerns regarding over-reliance on LPTA in the Department of Defense were addressed in the National Defense Authorization Act ("NDAA") for Fiscal Year 2017. The NDAA requires that "to the maximum extent practicable, the use of lowest price technically acceptable source

---

edge encryption technologies and should avoid policy initiatives that would have the effect of chilling such efforts.

[11] With regard to mobile device security specifically, we agree that layered mitigation strategies for the protection of mobile devices are critical and that they should include authentication that that is strong and, importantly, easy for the user to reliably use. To that end, the Administration should avoid overreliance on standards for authentication that would preclude the adoption of new technologies that offer security benefits. A flexible approach is critical to allow for innovative technologies that can enhance the user experience while reducing the likelihood that they will disable the authentication.

selection criteria shall be avoided when the procurement is predominately for the acquisition of information technology services" at the Department of Defense.[12] It also sets forth five conditions that the Department of Defense must meet before utilizing LPTA source selection criteria.[13] BSA believes that the same concerns that Congress addressed in the NDAA regarding overuse of LPTA source selection criteria within the Department of Defense may often arise in connection with IT procurements in other federal agencies as well. Accordingly, BSA respectfully recommends that the final version of the Report include language discouraging use of LPTA source selection criteria for procurements related to federal IT modernization.

B. Focus on Vendor-Supported Offerings

As already noted, BSA applauds the Report's recommendations that federal agencies actively seek to adopt commercial cloud services and other commercial offerings. As federal agencies increasingly purchase and "consume" IT resources as online services, rather than as products, however, it becomes more imperative than ever that federal agencies work with IT suppliers with a proven track record of offering robust and reliable support for their offerings.

Thus, we respectfully suggest that the final recommendations be more explicit in advising federal agencies to place a premium on selecting IT solutions for which the supplier (or some other commercial partner) offers reliable support.[14] This recommendation should apply equally to all IT solutions, regardless of licensing or development model. Doing so would be fully consistent with existing federal procurement rules, which encourage federal agencies to utilize commercially-supported products and avoid government-created boutique solutions. For example, the Federal Acquisition Streamlining Act ("FASA") of 1994 codified a preference for the acquisition of commercial items.[15] Similarly, the Clinger-Cohen Act expanded the preference for the acquisition of commercial items by significantly raising the threshold for the acquisition of commercial items and broadening the definition of commercial items.[16]

To maintain consistency with this policy, while also taking account of the current trend toward consuming IT resources as services, BSA urges the ATC's final version of the Report to

---

[12] National Defense Authorization Act for Fiscal Year 2017, H.R. 4909, 114th Cong. § 847 (2016) (enacted). Note that legislation that would apply the same requirements to the rest of the federal government has been proposed in the House of Representatives. *See* Promoting Value Based Procurement Act of 2017, H.R. 3019, 115th Cong. (2017).

[13] National Defense Authorization Act for Fiscal Year 2017, H.R. 4909, 114th Cong. § 847 (2016) (enacted).

[14] BSA likewise applauds the Report's recommendation for system deployments to be "automated to the greatest extent possible, removing the potential for errors caused by breakdowns in internal processes." Automating system deployments will enable agencies to customize features and provision devices for new users or environments in a cost effective and security enhancing manner.

[15] Federal Acquisition Streamlining Act, Pub. L. No. 103-355, 109 Stat. 3243 (codified as 10 U.S.C. § 2377).

[16] Clinger-Cohen Act, Pub. L. No. 104-106, 110 Stat. 186 (1996).

maintain its commitment to leveraging commercial IT solutions by recommending that federal agencies place a priority on selecting vendor-supported IT solutions.

C. Treatment of Legacy Systems

As the Report acknowledges, in order to modernize federal IT systems, some agencies may need to realign their current trajectory of IT investments. One of the Report's specific recommendations in this regard is that agencies "consider immediately pausing or halting upcoming procurement actions that further develop or enhance legacy IT systems identified that need modernization."[17]

While BSA recognizes that the process of modernizing federal IT systems may require halting certain procurement actions that are currently in the pipeline, we are concerned that the lack of guidance on how federal agencies should make such determinations could be interpreted broadly to create a presumption that software currently in use on existing federal IT systems is not worth continued maintenance or investment.

In our view, any such reading of the Report's recommendations risks placing federal agencies in a worse IT and network security posture than they are today. The mere fact that software is already deployed on an agency's IT system--even if it has been used for many years--does not mean that it is obsolete or in need of replacement as the system is modernized. The critical question is whether the software is secure and whether the vendor has continued to maintain and update the software to adapt to the agency's mission and changing requirements.

Additionally, BSA has concerns that encouraging federal agencies to "immediately halt" all planned investments in legacy systems might have the unintended consequence of creating lapses in vendor support for such systems--including critical security support. Automatically halting such procurements could potentially result in increased risk of security breaches or significantly reduced functionality during the time period while the legacy system is being evaluated and modernized.

BSA respectfully recommends that the final version of the Report provide more detailed guidance to agencies in evaluating both whether to replace their existing IT solutions and how best to maintain such systems until such time as they are replaced. In doing so, it might be appropriate to modify the existing guidance in the Report relating to the pace at which agencies decrease their current levels of support for such systems.

D. Funding for IT Modernization Efforts

As already noted, BSA welcomes the Report's recommendations to modernize and secure federal IT systems and the ambitious timelines that the Report sets forth for these efforts. However, BSA is concerned that the Report does not also urge Congress to provide additional funds to support this vital modernization effort. The Report suggests that "[a]gencies should also emphasize reprioritizing funds and should consider 'cut and invest' strategies that reallocate funding from obsolete legacy IT systems to modern technologies, cloud solutions, and shared services, using agile development practices where appropriate,"[18] and references The Economy Act, 31 U.S.C. § 1535, which authorizes interagency agreements for supplies

[17] *Report*, *supra* n. 1, at 4.

[18] *Id.*

and/or services, and agency-specific funding authorities.[19] In BSA's view, these passages fail to acknowledge the significant investments that may be necessary to update and modernize IT systems across the Federal Government, and also do not adequately explain how the reprioritization of funds and funding mechanisms will be able to underwrite the ambitious plans set out in the Report.

BSA encourages the ATC to support the Modernizing Government Technology Act ("MGT Act"),[20] which would establish a $500 million central fund for named agencies to pay for IT modernization over the next two years. The MGT Act passed the House of Representatives on May 17, 2017 and was attached to the Senate version of the National Defense Authorization Act, which passed the Senate on September 18, 2017. Additionally, BSA recommends that the final version of the Report include a more explicit recognition that modernizing federal IT systems may require substantial investments and calling on Congress to fund such efforts.

* * * * *

BSA appreciates this opportunity to provide these perspective on the ATC's draft Report to the President on Federal IT Modernization. We would be happy to answer any questions the ATC might have.

Sincerely,

Christian Troncoso
BSA | The Software Alliance

[19] *Id.* at 45.

[20] Modernizing Government Technology Act, H.R. 2227, 115th Cong. (passed by House, May 17, 2017).