PSC PROFESSIONAL SERVICES COUNCIL
The Voice of the
Government Services Industry

April 14, 2016

Mr. Tony Scott, U.S. Chief Information Officer & Administrator
Office of eGovernment and Information Technology
Office of Management & Budget
1650 Pennsylvania Avenue, NW
Eisenhower Executive Office Building
Washington, DC 20503

Dear Administrator Scott:

On behalf of the Professional Services Council (PSC), I am pleased to submit these comments on the proposed OMB guidance titled "Federal Source Code Policy – Achieving Efficiency, Transparency and Innovation through Reusable and Open Source Software" posted on the Federal CIO Council website for public comment. This guidance covers a number of important considerations on the acquisition of information technology (IT) solutions and it is crucial to reiterate the priority for commercial off the shelf (COTS) solutions and only developing custom code when absolutely necessary. When custom code is required, the final policy will need to identify necessary changes in contracting approaches as well as providing guidelines on when and how to best use open source software. It will be crucial to ensure that the guidance, and any subsequent Federal Acquisition Regulation (FAR) changes and related contract clauses, appropriately address issues of concern to contractors.

PSC is the voice of the government technology and professional services industry, representing the full range and diversity of the government services sector. As a trusted industry leader on legislative and regulatory issues related to government acquisition, business and technology, PSC helps build consensus between government and industry. Our nearly 400 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Through our Technology Council, we have ensured that the requisite expertise of our member companies and their employees are brought to bear on these vital IT challenges our government faces. Together, the trade association's members employ hundreds of thousands of Americans in all 50 states.

Focus on COTS first. We are encouraged that the first objective of the draft memo is to remind federal agencies to first consider shared services and commercial-off-the-shelf (COTS) solutions before embarking on custom-code development. However, the memo says very little about how to enforce this long-standing requirement. It would be helpful to include in the final memo a more specific up-front discussion emphasizing that custom code development should be the last resort, and that reliance on COTS wherever possible will not only allow government to take advantage of industry best solutions, but also force the crucially needed process optimization work that government agencies must address. An over-emphasis in the draft policy on custom code/open source without specific provisions on enforcing the preference for COTS will perpetuate allowing cumbersome and outdated processes to drive the need for custom code rather than relying on COTS to force much needed process change. In addition, given that custom coding should only be pursued when a need is so unique that it can't be met by the COTS solutions on the market, there may not be enough reuse opportunities to create viable open source communities.

Initial emphasis should be on incorporating provisions in new contracts. The memo focuses much of its content on a pilot process to make custom code already developed or under develop available for reuse and/or provided as open source software, and sets a target of requiring that 20% of custom code be released each year. Instead of measuring how much custom code is being released, which will be completely contingent upon the terms and conditions of the contract under which the code has been developed, the initial focus of the pilot should be on putting into place the right terms and conditions in new contracts for custom code that allow for appropriate release and reuse. By agreeing to terms up-front, government and industry will be aligned on the worth of the code being developed and will have a shared understanding of how that code will be used and reused. If a current contract for custom code requires that code be released, then agencies should be required to release the code. In those cases where current contracts don't provide for release and reuse, then the measure to be tracked should be how many new contracting actions providing for reuse are in place. In addition, measures of success for this pilot will need to recognize that (as noted below), not all custom code will be suitable for reuse or open source. In the near-term, capabilities like application program interfaces, utilities, file transfer components, application frameworks, and integration components may be good initial areas to focus on. An initial focus on the software components most likely to be reused would serve a better purpose than an across-the-board 20% target that measures the wrong behavior.

Seeking industry input on new contract provisions. It will be important to obtain industry input in advance of putting into place new contract provisions for custom code development and reuse. In some cases, a company may undertake the development of software for the government at a minimal profit with the expectation that they would retain rights for commercial distribution of the end product as a way to defray development costs and achieve their return on investment. Removing the right of commercial distribution may both reduce the number of companies interested in developing code for government and may also increase costs if the initial code development is priced to provide a stand-alone return on investment. Also, requiring reuse should not come at the expense of designing a solution that best meets the needs of the agency contracting for the work. Since custom coding by definition should be reserved for unique situations, the drive for potential reuse shouldn't force a "lowest common denominator" solution for the requesting agency without even knowing if additional demand for the solution exists in government.

Protection of current intellectual property rights. The policy's emphasis on releasing currently developed custom code does not include clear guidance on preserving intellectual property and derivative works rights for existing custom code. This issue argues for a revised focus on putting into place the right provisions in new contracts to address these concerns in advance of contract award. The policy should emphasize the continuing protection of existing intellectual property rights, as some companies may not want existing software to be moved to open source. The current FAR rights on technical data provisions also differ significantly from agency-specific data rights provisions, such as with DoD, NASA or the Department of Energy. These contract provisions should be acknowledged in any final memo and action directed to align them with the final OMB policy direction.

Not all custom code may be suited for open source. Open source software should be considered a viable source of supply for federal procurements, allowing agencies to choose between the best available proprietary and open source solutions. However, the policy memo should be clear that not all software requirements must be open source. There may be cases where mission critical systems and other sensitive software should not be put into the public domain, as is already recognized by the draft policy in regard to national security systems. When open source software has widespread applicability, and thus a broad and active support community, cybersecurity benefits can be obtained through review by a large number of users looking for vulnerabilities. On the other hand, if the user community for custom code is very small, or the software is for a sensitive mission or function, open source software may only introduce additional vulnerabilities. Broad distribution of sensitive source code may enable "bad actors" to identify and exploit

errors in released code with potentially damaging impact to government. Open source communities can thrive when there is sufficient marketplace demand for a specific open source product to justify their participants' investment of engineering resources. But, in the case of custom code without a broad application, the likelihood of an active open source community is diminished, minimizing the likelihood that other vendors would see a business rationale to invest resources in the continued maintenance and development of such a product. Without active and continuous user community review, more security risks than benefits may result. The guidance should point out that custom code only be considered for open source in those cases where there is a reasonable expectation that an active user community will be interested in supporting the effort. To this end, as noted above, rather than imposing arbitrary percentage targets for code release, agencies should be required to assess the viability of an open source marketplace before demanding custom code be open source, thus ensuring pressures to go open source don't over-ride security concerns.

Management requirements for open source need to be well understood. While there clearly are opportunities where open source software provides a viable solution for the federal government, care must be taken to not create additional cost burdens for government when an open source approach will require extensive management but little return. There are significant costs associated with managing both code reuse and open source software that, if not borne by an existing community or organization, would fall to the federal agency contracting for the custom code. When the user community for a custom code requirement is not significant enough to bear the costs and responsibility of code management, then forcing an open source solution would not be in the government's best interests. The policy guidance should therefore identify conditions that might encourage the viability of open source, e.g., large communities of developers with a common interest in the product, licensing terms which allow anyone to revise source code but that includes a mechanism for version control of the software (including patches, bug fixes, new features, etc.), active developer and user forums, etc. It would be far better for agencies to leverage existing communities rather than having to develop and nurture communities themselves. That said, it is encouraging that section 5.2 of the draft policy gives permission for formal participation in existing open source communities.

Licensing guidance needs to be provided. The policy should propose guidance on how to select the most appropriate open source software licensing arrangement. Recommendations should be given to agencies on the appropriate governance model to use for the open source project to ensure compatibility with government's intended use of the software. Additionally, licensing and contract language will still need to be developed to protect companies from future liabilities associated with code provided as open source.

Requirement for government to maintain an active role in open source code management. If the government wants to continue to receive the benefit from the code post-release, the government will have to maintain an active role (often referred to as "core-team" activity) in guiding the direction of future code evolution. Software developed for the government, particularly for citizen-facing services, may be subject to multiple requests for changes which will need to be addressed—requiring government commitment and cost. While the draft policy suggests that the government try to use existing communities to perform these activities, it must be recognized that, for some custom code requirements, existing communities may either not exist or may want to take the software in a direction incompatible with future government interests.

Code-of-conduct management. The extension of government interests into open-source software management may require enforcement of non-discriminatory evaluation of change requests and reported issues with released software. Agencies will need to ensure that code-of-conduct agreements have clarity and enforcement provisions to comply with government policies.

Identifying costs. As noted above, government may incur significant labor costs associated with administering and maintaining the structure of initially released government code as open-source, including naming conventions, account creation, software transfer, designation of applicable licenses associated with

code, and potential redaction activities. In addition to these administrative items, costs may also be incurred to produce suitable documentation, installation and configuration instructions, and explanations for the packaging of the source code. Costs associated with post-release activities may include governance, retention of government interest in software direction, evaluation of contributions to government code, establishing a roadmap for improvements/changes, development of code-of-conduct processes, and enforcement activities. These costs will need to be incurred to derive the full benefit from code released as open source. The policy should account for these activities and measure their costs during the pilot program to have full visibility into overall costs. This will help validate whether lower costs are being realized or if initial development costs are being offset by additional follow-on costs that were previously not captured. Indeed, sometimes indirect costs associated with implementation of open source software can be higher than those associated with COTS (e.g., staff training, change management, and updates and replacement).

Anti-Deficiency Act clarifications. The Anti-Deficiency Act has been clarified as not applicable to the acquisition of previously existing open-source software because such code was developed prior to any indication of government need, and as such was developed without any future expectation of payment. Clarity must be given in the final memo, since the draft policy states that code developed in response to specific government requirements will have been paid for prior to release as open source. In these cases, a reasonable expectation could be that future contributions to government developed open-source will also receive payment prior to being incorporated and released as open source. In other words, a company or individual may write and submit an enhancement to government open source software believing that such an enhancement is deserving of payment similar to original requirements. The final policy should be clear that contributions to government released open source will not be paid for even if original requirements were.

Background investigations on software developers. The draft policy proposes that public access be granted to government source code. This means that an individual, regardless of government clearance level (public trust or otherwise) may have access to and could contribute to government source code. The policy should be clear about how this will work alongside existing policies that require individuals to obtain clearances or suitability checks in order to work on government systems and software.

Privacy protections. Employees of contractors and government individuals creating source code for the government may not wish to have their personal information revealed via open-source change tracking systems. This could expose those developers to threats or unexpected insider exploitation. The policy should protect the individual privacy rights of developers working on such systems.

Transparency of requirements and architecture. The draft policy refers to the transparency of source code but is silent on the transparency of requirements that informed the architecture and implementation decisions for the source code created. Without access to these requirements and details of the architecture components, released source code may be subject to unnecessary, costly and unproductive debate defending and justifying decisions made. Yet, as noted above, care must be taken to not release details that would compromise sensitive solutions.

Relationship to other COTS/proprietary work. The policy should be clearer as to when a custom code requirement is for a unique or new feature inextricably linked to a proprietary/COTS solution. Solutions should not be arbitrarily broken into separate modules just to meet pilot thresholds for reuse; instead, the policy should identify how to determine whether the severability of code will allow for more reuse or instead will impact the proper functioning of the COTS solution and/or expose intellectual property. Many a government enterprise resource planning (ERP) effort has been hampered by the desire to customize rather than configure the ERP.

Scope of Pilot. A small, manageable pilot that targets putting the right contract language in place and establishing conditions for good decision-making should be the initial goal. The pilot phase would also be a

good opportunity to fully understand the costs and benefits associated with implementation. A more focused pilot would also allow for a faster identification of the impacts associated with contracting, releasing, managing, and maintaining open source software at a government agency. The work of the pilot phase could be divided into two simultaneous parts.

First, where current contract provisions already require code distribution and reuse, agencies should be told to make that code available. Open source software already in use should likewise be publicized. Second, a bounded pilot effort should focus on putting into place the right contract provisions and licensing terms, and then evaluate the costs and impacts of this approach. The pilot should focus on the types of widespread use and reusable components most amenable to open source collaboration. Special attention should be paid to understanding the cost and level of involvement necessary to ensure a viable open source community.

Identifying the right metrics for the pilot program will also be crucial. For open source projects, the effort should be evaluated to see if it has attracted and retained a viable community (as measured by the number of community members, number of issues and comments submitted, number of pull requests submitted and accepted, actual amount of reuse, etc.). In the end, there are a number of ways to involve open source communities in government work. Sometimes, it may be worthwhile to scan for existing open source solutions rather than forcing new code development to be done as open source. Again, the primary goal should be to leverage existing solutions (COTS or open source) rather than embarking on custom code development in the first place.

Thank you for the opportunity to comment on this policy. PSC would be pleased to discuss our recommendations with you and others. In the interim, please feel free to contact me by email at wennergren@pscouncil.org or by phone at 703-778-7557, if you have any questions or need additional information.

Sincerely,

David M. Wennergren
Executive Vice President, Operations & Technology