IT Alliance for Public Sector
A Division of ITI

April 11, 2016

The Honorable Tony Scott
Federal Chief Information Officer and
Administrator for E-Government and Information Technology
Office of the Federal Chief Information Officer
Office of Management & Budget
1650 Pennsylvania Avenue, NW
Eisenhower Executive Office Building
Washington, DC 20503

RE: OMB Draft *Federal Source Code Policy – Achieving Efficiency, Transparency and Innovation through Reusable and Open Source Software*

Dear Mr. Scott:

On behalf of the Information Technology Alliance for Public Sector (ITAPS) [1], we are responding to the request for comments regarding the Office of Management and Budget (OMB) the *Federal Source Code Policy – Achieving Efficiency, Transparency and Innovation through Reusable and Open Source Software*, released on March 10, 2016. The proposal sets forth guidance to covered agencies regarding acquisition policy governing custom software procurement by the government, establishes policy requirements for government-wide source code receipt and reuse, and creates requirements for releasing code under an open source license. ITAPS appreciate this opportunity to share our perspectives and comment on these draft guidelines.

With the federal government relying increasingly on information technology (IT) and software solutions as a central element to carrying out its missions and business functions, we understand OMB policy efforts to address software. There are some areas that ITAPS supports in the proposal, while others we recommend changes or the need for OMB to clarify. Generally speaking, we have concerns about the ability of the government to effectively sustain an open source code policy. It is not because agencies would not choose open source code as an option when acquiring software, but that federal agencies are inadequately resourced with the requisite technical expertise to effectively modify and integrate such code into their unique mission needs. These resource shortcomings are only exacerbated by the relentless and necessary updating of software code that would make the adoption, integration and sustainment of an open source code policy challenging in the government market. Please find below our specific comments and concerns.

---

[1] **About ITAPS**. ITAPS, a division of the Information Technology Industry Council (ITI), is an alliance of leading technology companies building and integrating the latest innovative technologies for the public sector market. With a focus on the federal, state, and local levels of government, as well as on educational institutions, ITAPS advocates for improved procurement policies and practices, while identifying business development opportunities and sharing market intelligence with our industry participants. Visit itaps.itic.org to learn more. Follow us on Twitter @ITAlliancePS.

Software Procurement Consideration: Commercial-off-the shelf Software

We strongly support the government's intent to continue leveraging commercial off-the-shelf (COTS) technologies, which have been the preference for the federal government for more than twenty years, along with existing federal software solutions. We believe this approach, providing "preference to existing federal software solutions (e.g. federal shared services or existing reusable code) or a purchasable off-the-shelf software solution (e.g. [including] COTS)" is sufficient, but may have been poorly enforced, if enforced at all in the past. That is why we may see federal agencies assume that their technology needs are as different from those of private sector enterprises as to justify the procurement of custom solutions. We believe that without an enforcement mechanism, this requirement will remain insufficiently observed. We recommend that agencies be required to notify OMB of any decision to procure a custom solution, and that the agency in question be required to justify why it needed to procure such a custom solution.

The draft states at footnote 2 that "the term 'COTS' also generally encompasses commercial item solutions." While we do not oppose this more expansive application of the definition, it is the obverse of the definition provided in Federal Acquisition Regulation (FAR) 2.101, where "COTS" items are a subset of "commercial items."

Our members are concerned with the lack of clarity around the meaning of "custom code" in the proposal. While some federal procurement contracts lead to the custom development of an entire IT solution, it is customary for a software vendor to customize its commercial code for government purposes. That vendor, and the commercial market in general, considers such customization to be a minor modification to a commercial product, consistent with FAR Part 2.101. Thus, both the commercial code and the custom modification are subject to the applicable commercial license agreement. The draft open source policy, however, does not set out a definition of what constitutes custom code, and it raises significant concerns over whether contractors will be asked to give rights to their commercial source code and to its valuable commercial, intellectual property (IP). Moreover, to the extent that the government seeks to limit IP rights based on such customization, it would be acting outside the norms of customary commercial practice, raising government contract law concerns. The government has a statutory obligation to ensure that its requirements are set forth to allow commercial items to fulfill them to the maximum extent practicable, and, generally, it must ensure that its terms and conditions align with customary commercial practices.

It is not clear how this policy will affect the custom development of a new feature of an otherwise propriety commercial product at the request of an agency. The proposal seems to apply to not only entire products that are custom developed for agencies, but also to modules and add-ons that are self-contained. OMB should clarify that this policy does not apply to custom features that are not separable from the underlying COTS product. Our concern is that should agencies require contractors to put such custom features into modules, contractors' core IP would be exposed. Along these lines, the phrase, "In the performance of a federal agreement," is quite broad, certainly broader than a federal agreement for the development of software. This breadth could have IP and security implications, and it could present a barrier to small businesses seeking to participate in the government market because they are forced to give "unlimited rights" to the government. The Exceptions section might cover security, but it appears

silent on any IP rights that might co-exist with the code developed in connection with the procured commercial software. ITAPS believe that this issue needs to be resolved.

Other elements of the policy regarding the use of COTS that need further elaboration and clarification include:

a) The need to recognize that some software might not be COTS, but can be a commercial item. OMB should clarify that non-COTS commercial items are excepted from review under this policy.
b) Specifying that the term COTS includes perpetual, subscription, and term software, to name a few.
c) When and under what conditions updates and upgrades to COTS are covered by the Policy.
d) Ensuring that COTS technical support is not covered, even if initiated at the request of Covered Agencies and whether done by the licensor of the COTS software or on its behalf.
e) Specifying what constitutes "professional services" in connection with COTS software and whether or not they are covered by the Policy.
f) Whether or not the Policy requires ownership, and:
    i. Clarification that the Policy does not prohibit the Covered Agencies from licensing back the custom code to the party that developed it so that party can re-use it with other customers.
    ii. Clarification that the code ownership is for the copyright and not to any other IP like trademarks, trade secrets or patents.
g) Whether or not a broad license to use by all Covered Agencies may suffice.
h) The ability of the developer has the right to negotiate other commercial terms like limitation of liability, IP defense and indemnification, etc.

Government-Wide Code Reuse

Objective 3 in the draft policy distinguishes public domain access from the formal licensing that defines OSS. Later in the section on "Government-wide Code Reuse," it is noted that "although Government-wide reuse of custom-developed code shares some of the same benefits as OSS, it does not meet the definition of OSS and should therefore not be mislabeled as such." Given this recognition, these comments will focus on achieving the objective as it relates to OSS. We would like to call to your attention to several policy elements related to licensing and other protections of software, including OSS as part of custom code, that pose challenges to the implementation of the policy as stated.

We would disagree with the assertion at lines 147 – 148, which states that software "created on behalf of the Government by third parties, such as private sector vendors, is subject to copyright protection." Such a statement might lead some uninitiated vendors to believe that they would be able to retain copyright protections on software under this policy. Such a claim is misleading and inaccurate. Under FAR 52.227-14 or DFARS 252.227-7014, where the government has unlimited rights in software that is first produced in the performance of the contract (except for minor modifications of pre-existing proprietary software). Even though the contractor could put its copyright notice on the software, that notice would not override the broad unlimited rights the federal government already receives under existing contract law.

Delivering source code with unlimited rights, as outlined at lines 157 – 174, could also be challenging for contractors who wish to use the source code in their products, in terms of maintaining various versions, incurring infringement liability, and other risks and liabilities. If government agencies want the ability to reuse and modify, then it will become very difficult and/or expensive for the contractor (or anyone else) to provide maintenance support for it. Consequently, this element of the policy could have the opposite effect by increasing cost for the federal government. The federal government should assume that contractors will charge a premium to the first agency to acquire the code to compensate for the fact that they can only charge for the code one time. The savings for the government are supposed to come from the fact that reuse would be free, however, such reuse may not happen (and is in fact unlikely, since the code was custom-developed because no vendor expected much, if any, commercial demand for it), and so there may be no savings.

The language found at lines 162-164 regarding "secure unlimited rights to the custom source code" also poses challenges. In addition to the concerns previously raised, OMB should be aware that, to the extent the custom source code includes OSS, some OSS licenses provide for automatic termination of the license if the licensee breaches a term of the license. One open source license has a retroactive termination provision. Therefore, such custom code which includes other OSS elements, upon reuse anywhere across the federal enterprise, would potentially invalidate the license for those elements and trigger additional liabilities. Furthermore, the language at line 174 states that the agency shall "make custom-developed code available to all other federal agencies." OSS licenses are vague as to which entity constitutes the "licensee." Some open source licensors take the position that transferring OSS from the licensee to a sister company constitutes a distribution and is not usage of the OSS for internal purposes. Therefore, "mak[ing] custom-developed code available to all other federal agencies" may trigger OSS licensing provisions and undermine the policy intentions. These and other licensing limitations on OSS when used as part of custom-developed software should be addressed by the policy before finalization.

The proposed policy requires that those agencies that procure new custom code whose development is paid for by the federal government make that code available for reuse across federal agencies and that a portion of that new custom code be released to the public as Open Source Software (OSS). The policy defines custom code as "software source code that is written to fulfill a specific purpose that is not already addressed by existing programs or COTS solutions. For the purposes of this policy, custom code development must be fully funded by the federal government and is either developed by a contracting entity for use by the federal government, or developed by covered agency employees in the course of their official duties." We believe the policy should be clear that the requirement to re-use custom code applies to code that was specifically developed and paid for in its entirety by the federal government, and not to cases where a portion of the development costs are not attributable to the government contract.

Finally, we would note that elements of the policy would seem to direct contradictions to the narrative of this Administration to attract new companies with potential for new innovations into the federal government vendor base. The policy requires the government to "secure unlimited rights to the custom source code, associated documentation and related files – which includes the right to reproduction, reuse, and distribution of the custom source code, associated documentation and related files across the

government." Unlimited rights mandated by the Federal Acquisition Regulation for government-financed software, however, are frequently identified as a direct impediment to participation in the government market by innovative and cutting edge technology firms. As part of the implementation of this policy, we encourage the continuation, by various government entities, of examining whether the current Rights in Technical Data requirements should be more narrowly tailored to accelerate the engagement of commercial companies who depend upon their intellectual property rights to be successful. To further lessen barriers to the federal market, we would also encourage the development and publication of best practices along with standard contract and service level agreements to ease the compliance burden on contractors related to these requirements.

Open Source Pilot Program

Most ITAPS members support limited policy implementation as a pilot program. We would encourage the government to take the time the policy is implemented in a pilot program to address and resolve the challenges noted above and to identify additional challenges. OMB should use the piloting period to assess whether the various policy elements are feasible and are being successfully adopted and implemented and to catalog best practices where they may emerge for sharing with other agencies as the policy matures. We would also encourage the development of metrics to measure several of the assumptions and premises of the policy, like whether or not a robust community will spring up and be sufficient to support OSS for all software developed using government funds. If an insufficient community arises to support the publication of 20% of federal government custom code, then plans to expand the policy to more or all custom code should be deferred.

Definitions

The policy should clarify the status of derivative works and offer a clear definition of the term in relation to previously non-open-sourced code. If a contractor brings source code IP to the government as part of a solution, and the government directs the contractor to perform customizations on the code, it is unclear how such customizations could be released as open source code in a manner that protects the original IP. The policy should be amended to include protections on previously existing IP so that contractors can be confident of retaining rights to pre-existing software. Many vendors will not be interested in licensing their existing software to allow it to be open source to all agencies and the public.

As noted above, all of our members expressed concerns regarding the lack of clarity around the definitions of "custom code" and "mixed code." We are not sure if this policy covers code that is developed in the normal course of implementing commercial software, e.g., to permit commercial software to interface with legacy systems. Much of what is developed under federal contract is mixed code, where the contractor is modifying proprietary software. This is currently addressed in the DFARS under Government Purpose Rights, which seems to work fairly well. If the draft policy, however, is stating that all custom code should be either OSS or otherwise be fully available to all federal agencies, then that is going to impact how contractors approach pricing and risk allocation and will undoubtedly lead to many possible competitors to forego federal government contracting. OMB should consider including the downstream

effect on contractors and the software community in general in the policy, including requirements to train contracting officers in the tradeoffs that contractors will seek and how to address them.

Tech Neutrality in Implementation of Open Source Policy

ITAPS strongly supports technology neutrality in any product selection for IT goods and services for which the government may contract, so we appreciate the inclusion of instruction to agencies to adhere to the requirements of OMB's Technology Neutrality memorandum dated January 7, 2011. Several companies, however, do not see how an open source policy and the tech neutrality policy are compatible. We would encourage additional clarification on such compatibility and how a government-wide open source policy could not substantially depart from the spirit and letter of that memo.

In addition to clarifications that the implementation will not violate the tech neutrality memo guidance, OMB should also take steps to re-state the provisions of FAR Part 11.104 and 105 to clearly identify for agencies and those managing the implementation of the policy that they should not specify particular brand names in the course of identifying platforms and products with which to create open source code. Too frequently, companies have experienced preferences for particular products in those open source efforts already underway. We believe that, as in all government procurements, there should be a strong effort to sustain technical neutrality in the types of products that might be chosen to fulfill the open source requirements and that agencies should not specify products except under the provisions afforded through FAR Part 11.104 and 105.

Security

The language at line 409 regarding the reference to an "identifiable risk" to the "security" of the agency's systems would seem to be the only policy reference that addresses the issue of the security of OSS, though this language doesn't address the issue head-on. The quality and safety of open source software depends upon a robust community evaluating and testing software code on a continuous basis. This is a factor of market forces: where there's sufficient market demand for a product, there's a community of users and developers/vendors that supports the products. If there's a weak demand, there will not be a community. If there are only a few agencies that might reuse code developed previously as custom code, that level of demand has not previously proven to be sufficient to sustain the necessary community of users to adequately and continuously review, refresh and update the code. Without a community to continuously review and maintain it, especially if it's mainly used by the government, the code becomes stagnant and vulnerable to exploitation. Any decision to open source custom code must be driven by clearly defined mission needs and include clear and credible commitments from an existing open source community, not merely to host the code and make it available to contributors, but to actually continue its development, maintenance, and security patching.

Cloud Offerings

With federal agencies moving more applications and data to the cloud, we need to understand the impact of this policy on cloud computing offerings. OMB needs to clearly state that this policy does not apply to cloud computing, i.e. to Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) custom code. OMB should also clarify that, if the software is delivered by a cloud service, the terms and conditions of the cloud delivery portion of the "bundle", including pricing, are outside the scope of this draft.

Anti-Deficiency Act Clarifications

While the Anti-Deficiency Act has been clarified as not applicable to the acquisition of previously existing open-source because such code was developed prior to any indication of government need, and as such was developed without any future expectation of payment, this policy may not be as clear. Since the policy states that code developed in response to specific government requirements will have been paid for prior to release as open source, a reasonable expectation could be formed that future contributions to government developed open-source will also receive payment prior to being incorporated and released as open source. In other words, an actor 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 policy may need to be amended to be clear that contributions to government released open source will not be subject to remuneration, even if original requirements were so compensated.

Resource Clearances

This policy is proposing 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 certifications, undergo government mandated training and retraining and clearances to be able to access and work on government systems and software. The public access afforded under this policy to software code intended to be used and reused on government networks would seem to directly contradict these personnel security requirements.

Unaccounted for Costs

As one of the policy's main objectives is lowering of costs associated with government software procurement, the government may want to consider implementing control functions into the policy to address the long term maintenance costs associated with releasing source code as OSS. The policy should also identify and put in place effective means to measure these additional costs associated with the use of OSS that will be borne by the taxpayer. Examples of such costs include:

i. The labor 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 there is the effort to produce suitable, distributable

documentation, installation & configuration instructions, and explanations for the packaging of the source code. This information is critical to understanding how the source code can/should be used or is being used.

ii. Stewardship labor associated with post-release activities including 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. Costs associated with (ii) can be non-trivial and may be necessary to continue to obtain benefit from code released as open source. Examples include:

- Maintaining an active role. If the government wants to continue to receive benefit from the code post-release, the government will have to maintain an active role (open-source often refers to this as "core-team" activity) in guiding the direction of code evolution through approving or denying change requests to the source code (via review of "pull requests"). Systems related to government mission activity, particularly benefits, may be subject to high levels of requests for changes, which will need to be addressed, and may require transparent "equal-access" style debates. The labor required for these efforts will need to be funded. While the policy suggests that the government use "existing" communities to perform these activities, doing so may result in higher probability that the communities may 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. Existing code-of-conduct agreements may lack clarity and enforcement provisions that comply with government policies. Taking an active role in such activities will require the government to allocate labor costs associated with proper definition and enforcement of well-defined practices.

The government should amend the proposed policy to account for such activities and measure their costs during the pilot program to have full visibility into overall costs. This will help validate whether the lower costs are being realized or if initial costs are being offset by costs that were previously not captured.

Applicability to Grants and Cooperative Agreements

OMB sought feedback in whether this draft policy should be applicable to grants and cooperative agreements, which includes state and local governments, universities, non-profits and other entities that receive federal funding. The GSA component 18F has vocally supported the extension of this policy to state and local programs that utilize federal funding through grants, cooperative agreements and federally supported benefits programs.

We have seen situations where a state procuring technology using its rules, incorporates its interpretation of federal intent flowing from these rules. The reality in state government is well-reflected in the often repeated statement "if you have seen one state system, you have seen one state system".   Other than a few possible examples, states' design and operate their programs very distinctly and specifically for a

variety of reasons that include, among other things, political environment, budget-related forces, population factors, economic climate, etc. We don't imagine a time when a state government would simply "download" source code from a federal repository so that they can implement a new state system. Although the source code may be a starting point (of some sort), the state would require significant resources to customize the code to meet their specific program design. It has been the experience of our member companies that such customization is significant and ever-evolving.
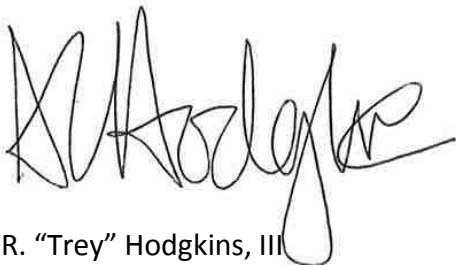
Moreover, we foresee a situation where the states would have a very difficult time contracting to use the open source code. As most states do not have the internal resources to implement open source code, they would turn to contractors to integrate the code into the existing systems in each state. In such a contract, we would anticipate that the states would attempt to push most, if not all, of the risk to the contractor and most experienced contractors would not accept such risk. For those contractors that did accept the risk, the cost would most likely be so prohibitive as to eradicate any anticipated savings for the government from the open source concept.

We do believe that the open source concept has limited possibilities for utilization in specific areas such as business rules development. As an example, once the Supplemental Nutrition Assistance Program (SNAP) rules are built, they could be shared with any state that was interested in deploying the same product for determining SNAP eligibility. But the core case management structure of a state system will remain a highly customizable piece of business that will require the states to contract with experienced software developers and systems integrators for delivery, even despite the possible availability of open source code.

Conclusion

Thank you again for the opportunity to respond to this request and share our viewpoints. We encourage the federal government to continue to promote the preference for COTS products in acquisitions in compliance with the law and ensure that any open source code policy requirements are set forth to allow commercial items to fulfill them to the maximum extent practicable, and ensure that its terms and conditions align customary commercial practices. We look forward to working with OMB as this policy is refined, and we are available at any time to elaborate on our response. Should you have any questions regarding these comments, please contact Pamela Walker, Senior Director of Federal Public Sector Technology at (202) 626-5725 or pwalker@itic.org.

Respectfully Submitted,

A.R. "Trey" Hodgkins, III

Senior Vice President, Public Sector