April 11, 2016

Tony Scott
Administrator and Federal CIO
Office of Management and Budget (OMB)
725 17th Street, NW
Washington, DC 20503

Subject: Federal Source Code Policy–Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software

Dear Administrator Scott,

Thank you for the opportunity to provide comments in response to the draft *Federal Source Code Policy – Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software*. The Coalition for Government Procurement sincerely appreciates the opportunity to review and provide input to OMB on the draft policy.

The Coalition for Government Procurement ("the Coalition") is a non-profit association of firms selling commercial services and products to the Federal Government. Our members collectively account for a significant percentage of the sales generated through General Services Administration ("GSA") contracts including the Multiple Award Schedules program. Coalition members are also responsible for many of the commercial item solutions purchased annually by the Federal Government. Coalition members include small, medium, and large business concerns. The Coalition is proud to have worked with Government officials for more than 35 years towards the mutual goal of common sense acquisition.

The Coalition supports overall efforts by OMB to fuel innovation, lower costs, and benefit the public through the use of technology, including open source software. The Coalition, however, has a number of concerns regarding the proposed policy, namely use of the term "commercially available off-the-shelf" versus commercial item, the protection of intellectual property rights, consistency with OMB's technology neutrality

policy, security assurance for agency released code, and the artificial mandate requiring the release of 20% code.

COTS vs Commercial Items

Throughout the draft policy, the term "commercially available off-the-shelf" or COTS item is used to refer to commercially available software that is developed and owned by private companies or developed and licensed as open source. In addition, Footnote 2 of the draft states that for "purposes of this policy, the term COTS also generally encompasses commercial item solutions." The use of these terms in the draft, however, are inconsistent with current statutory requirements and their definitions[1] in the Federal Acquisition Regulation (FAR).

Paragraph 3 of the Federal Source Code policy would misapply current statutory requirements for giving preference to the acquisition of software that qualifies as a "commercial item," as opposed to the policy's use of the term COTS software. Section 3307 of title 41 U.S.C. and sections 2375-2377 of 10 U.S.C. clearly establish a preference for the acquisition of commercial items, not a subset of commercial items.[2] Thus, any policy in this area should align and comply with that statutory mandate rather than seeking to redefine it as a preference for COTS software.

In addition, the Coalition recommends that the policy utilize the term "commercial item" rather than COTS in order to ensure that the intellectual property rights of companies that have invested in the development of software qualifying as a commercial item, and not just "COTS," are protected, particularly when licensing terms are addressed. Section 12.212 of the FAR already establishes clear guidance for agencies in negotiating license terms for commercial item software. The policy should clearly acknowledge this regulatory guidance, which implements and has the force and effect of law. Further, use of the term "commercial item" would bring the policy more in alignment with the Administration's critical objective of fueling innovation because,

[1] The FAR defines "commercial item" at 2.101 as any item that is of a type customarily used by the general public or by non-governmental entities for non-governmental purposes, and has been sold, leased, or licensed to the general public (or offered as such). "Commercially available off-the-shelf (COTS) items" are defined in FAR 2.101 as a subset of commercial items. COTS items are generally defined as a commercial item that has been sold in substantial quantities in the commercial marketplace and offered to the Government in the same form in which it was sold in the commercial marketplace.

[2] Indeed, unlike the approach taken in the proposed Federal Source Code policy, the statutory preference for the acquisition of commercial items "goes in the other direction." Rather than narrowing the government's focus on a subset of commercial items, to the extent that suitable commercial items are not available, there is a preference for nondevelopmental items other than commercial items. *Cf.* 41 U.S.C. 3305, 10 U.S.C. 2377, and 41 U.S.C. 110.

unlike COTS items, commercial items are not limited to those that have already been sold in substantial quantities in the commercial market.

Intellectual Property Rights

The Coalition notes that, with regard to custom software, the development for which the Government pays, the policy addresses issues for which the Government's existing rights already are well-established. The FAR has long-established that the Government obtains "unlimited rights" in "[d]ata first produced in the performance" of a contract for non-commercial items. FAR 52.227-14. The term "data" includes "technical data and computer software." *Id*. The term "unlimited rights" means "the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so." *Id.* The Government also has the ability to require contractors to identify computer software that will be delivered as software with less than unlimited rights so that the remaining software delivered is delivered with unlimited rights. *See* 52.227-15. Thus, in light of the Government's existing rights, the policy should be limited to referencing acquiring software and IP rights consistent with the FAR.

In addition, the policy's section on Exceptions to Government-wide Reuse or to Publication unequivocally should respect the intellectual property rights of the developer for code developed in connection with procured commercial software, consistent with commercial practices. Development activities, including tailoring, customizations, add-ons, and other development are customary commercial activities associated with the acquisition and implementation of commercial item software. Failure to safeguard vendors' intellectual property rights (and otherwise opening their products) simply because they engage in these customary commercial activities risks undermining their core investment, if not their overall business, and raises security concerns that need to be investigated and understood. Rather than attract innovative firms into the government market—a declared objective of the Administration—these risks could present an insurmountable barrier to their entry.

Moreover, lack of clarity around vendors' intellectual property rights in this regard can affect the ability for the government to solicit, and vendors to offer, commercial solutions for agencies under contracts. It should be recalled that the Federal Acquisition Streamlining Act of 1994 (FASA) requires agency heads to ensure, to the maximum extent practicable, that commercial items may be procured to fulfill agency requirements, that requirements be modified so they can be met by commercial items, that specifications be stated to enable offerors to supply commercial items, and that policies be revised to reduce the impediments to acquiring commercial items. See 41 U.S.C. 3077. FASA is implemented at Part 12 of the FAR. FAR 12.212 (a) provides

that the government shall acquire software under commercial license terms, and FAR 12.301(a) specifically provides, in part, that "contracts for the acquisition of commercial items shall, to the maximum extent practicable, include only those clauses required by law or *"[d]etermined to be consistent with customary commercial practice*." [Emphasis added.] Further, FAR 12.302(c) precludes the inclusion of any term or conditions in a solicitation or contract for commercial items in a manner *that is inconsistent with customary commercial practice for the item being acquired unless a waiver is approved in accordance with agency procedures*." [Emphasis added.]

In light of the foregoing, and consistent with governing law, we recommend that contractor intellectual property rights be included in the list of applicable exceptions in which the release of the code would be restricted, including explicitly, intellectual property rights for code developed in connection with procured commercial software.

Technology Neutrality

The Coalition is concerned that the proposed draft and the Software Procurement Analysis (Appendix B) are inconsistent with OMB's current policy of technology neutrality. The draft policy seems to establish a distinction between open source software, which is an industry-recognized licensing model, and custom software development. The Federal Source Code Policy should not, through repeated use of the term, establish a preference for open source software versus proprietary software developed exclusively with private funds.

Selection of the most appropriate software solution for an agency should be based on the particular needs and requirements unique to that agency. How the technology is developed, licensed, or distributed is secondary to the ability of the technology to meet an agency's requirements. The OMB *Technology Neutrality* memorandum released on January 7, 2011 states that "as program, IT, acquisition and other officials work together to develop requirements and plan acquisitions, they should follow technology neutral principles and practices." Although the draft policy does recognize the established government-wide technology neutrality policy currently in effect, its focus presents custom developed software's only alternative as open source software. That is not the case. Software developed for and paid for by the Government need not be Open Source Software in order to achieve the overall intent of the policy which appears to be to make sure the Government receives full value and benefit for its investment in custom software development.

Open Source Communities

The draft policy encourages agencies to release code in a manner that fosters communities, optimizes opportunities for these communities to provide feedback on and contribute to the code, and encourages Federal employees and contractors to get involved in open source projects. Open source communities, however, are not generated top-down. Rather, they respond to already existing demand for certain solutions. Where this demand exists, there is likely a group of developers/vendors who are willing to invest the time and effort in developing such a product. The Coalition is concerned that the proposed pilot's open source software release of 20% of custom code may not stimulate open source communities, as assumed by the proposed policy, if there is a lack of demand.

Requirement to Release 20% Custom Code

The artificial mandate to release 20 % of custom developed code each year is an unrealistic goal that will create problems, as agencies focus on meeting the goal rather than focusing on ensuring that the Government is better able to utilize already existing rights in custom developed software to fulfill their missions. Resources would be better spent on educating the Government procurement workforce rather than tracking goals that will encourage the release of software that could, in fact, create more security risks than public benefits and otherwise undermine competition based on barriers to market entry, as discussed previously in relation to IP rights. In addition, it is unclear what quantity and type of software could be spawned in this process and whether and how the Government might need to manage this output. Likewise, it is not clear what obligations would exist for the developers of such code, or what the implications would be for the vendors of those products that interact with such code.

The policy also emphasizes quantity goals over the quality of software to be included in the repository. Government officials should be encouraged to work with each other and private industry to identify and prioritize the type of software that is to be placed in repositories rather than focusing on an artificial goal.

Security Concerns

The Coalition is highly concerned that the pilot program does not provide Federal agencies with the robust guidance necessary to protect the security of any released code. It is absolutely critical that any open sourced code be utilized by active and engaged open source communities. Without the continuous attention of active communities, the open sourced code released by the U.S. Government could be vulnerable to malicious hackers. Releasing custom code without a committed open source community would be a major cybersecurity risk for Federal agencies mandated to release code under the Federal Source Code Policy.

Again, the assumption that open source communities will respond to the release of agency code is a major flaw of the proposed policy. Our members report that, outside the Government, these communities operate when there is significant demand for a specific open source product and there are entities and individuals that are willing to invest their engineering resources in these projects. The release of custom code by the government, however, may only be of interest to the original agency or a small group of agencies. Such a small number of potential customers is unlikely to incentivize vendors to invest the resources necessary to support the code, creating a significant cybersecurity risk for the Federal Government. *OpenSSL* is a real example that demonstrates that the lack of active community engagement leaves open source code susceptible to malicious hackers who may be the only ones interested in testing to exploit weaknesses in the code.

It is critical to our nation's security that the Federal Source Code Policy provide more specific guidance to agencies about how to protect released code. The policy should require that prior to the release of any code, the agency Chief Information Officer (CIO) ensure that an active open source community is planning to invest in and take continuous responsibility for the code. Further, the agency CIO should document this. These steps will provide greater security protection to Federal agencies by ensuring that a genuine plan is in place for an open source community to support and secure code.

Questions

The Coalition requests that clarification on the following questions be provided prior to the issuance of the final Federal Source Code policy:

1. Objectives (pg 3): The draft states that the guidance "applies only to software developed in the performance of a Federal agreement." What IP and security implications would this language have? What IP rights might co-exist with the code developed in connection with the commercial software procured? What is the intent of the phrase "in the performance of a Federal agreement?" How is the phrase "in the performance of a Federal agreement" the same or different from the phrases "pursuant to a Federal agreement" or "under the terms of a Federal agreement?"

2. Scope and Applicability (pg. 3): The draft states that the policy's requirements apply to all covered agency agreements for Federally-procured software including "requirements for, *or may result in*, custom-developed code." [Emphasis added.]

    a. Would coding that is customary in the implementation of a commercial shrink-wrap solution also be covered, and if so, in light of the fact that such coverage would conflict with

existing law and customary commercial practices, and otherwise undermine Government market participation by innovative companies, why?

b. How would the policy affect the custom development of a new feature of an otherwise proprietary commercial software product requested by an agency, and if it does affect such custom development, in light of the fact that such coverage would conflict with existing law and customary commercial practices, and otherwise undermine Government market participation by innovative companies, why?

c. How would the policy apply to modules and add-ons that are self-contained and if it does affect such modules and add-ons, in light of the fact that such coverage would conflict with existing law and customary commercial practices, and otherwise undermine Government market participation by innovative companies, why?

d. How would the policy apply to custom features that are not severable from an underlying commercial software product and, in light of the fact that such coverage would conflict with existing law and customary commercial practices, and otherwise undermine Government market participation by innovative companies, why?

3. Definitions (pg. 13): Does the custom code definition cover code that is developed in the normal course of implementing commercial software (*e.g.,* to permit commercial software to interface with legacy systems), and if it does affect such development, in light of the fact that such coverage would conflict with existing law and customary commercial practices, and otherwise undermine Government market participation by innovative companies, why?

Thank you for the opportunity to review OMB's Draft Federal Source Code Policy and provide public comments. If you would like to discuss any of these topics further or have any questions, please contact me at (202) 331-0975 or rwaldron@thecgp.org.

Sincerely,

Roger Waldron

President