The Software Alliance

BSA

April 11, 2016.

Anthony E. “Tony” Scott
Administrator and Federal Chief Information Officer
Office of E-Government and Information Technology
Office of Management and Budget
1650 Pennsylvania Avenue, N.W.
Washington, D.C. 20502
Via sourcecode@omb.eop.gov

Dear Administrator Scott:

Comments on Proposed Federal Source Code Policy

I. Introduction

BSA | The Software Alliance (“BSA”)[1] welcomes this opportunity to comment on the OMB’s proposed source code policy for software that is custom-developed for the Federal Government (“Source Code Policy”).[2] These comments are informed by decades of experience and deep expertise in areas that lie at the heart of the Source Code Policy.

BSA’s member companies include the world’s leading developers of software and other information technology (“IT”) products and services, many of which are IT partners with Federal agencies that would be subject to the proposed Policy.[3] These companies collectively invest tens of billions of dollars annually in developing software, and they distribute software under a wide variety of licenses, including as open-source software (“OSS”), as proprietary software, and as mixed-source solutions. BSA and its members

[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 around the world, 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.

[2] OMB, *Federal Source Code Policy—Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software* (March 2016), available at https://sourcecode.cio.gov/SourceCodePolicy.pdf.

[3] BSA’s members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, Dell, IBM, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro and Workday.

recognize that customers have varying needs, and we champion policies that give customers—including government customers—the freedom to select and use whichever type of IT product, service, or development or licensing model best suits their needs.

BSA supports this Administration's efforts to improve, streamline, and strengthen Federal IT practices, including its guidance favoring the use of cloud computing,[4] promoting open data and data interoperability,[5] increasing shared approaches to IT service delivery across Federal agencies,[6] endorsing technology neutrality,[7] and strengthening IT security.[8] We also support the Source Code Policy's objectives of ensuring that Federal IT procurement practices promote cost efficiency, increase transparency, and improve citizen experiences with core Government programs.[9] We offer the following comments in hopes that they will advance the objectives set forth in these and other recent Federal IT policy documents and directives.

II. Overview of Proposed Source Code Policy

As drafted, the proposed Source Code Policy directs covered Federal agencies wishing to procure software to undertake a three-step analysis:

- First, the agency must determine whether its needs could be met by an existing solution for which the Government already holds appropriate license rights, including Federal shared services or previously developed software available for reuse. If such solution exists, the agency should use it.[10]

- Second, if no such solution exists, the agency must determine whether an appropriate commercially available off-the shelf ("COTS") solution is available.[11] In undertaking this analysis, agencies must consider "proprietary, open source, and mixed-source software

[4] *See, e.g.*, The White House, *Federal Cloud Computing Strategy* (Feb. 8, 2011), available at https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

[5] *See, e.g.*, OMB, *Memorandum on Open Data Policy—Managing Information as an Asset* (May 9, 2013), available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf.

[6] *See* OMB, *Memorandum on Increasing Shared Approaches to Information Technology Services* (May 2, 2012), available at https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/sharedapproachmemo_0502.pdf.

[7] *See* OMB, *Memorandum on Technology Neutrality* (Jan. 7, 2011), available at https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf.

[8] *See, e.g.*, OMB, *Memorandum on Enhancing the Security of Federal Information and Information Systems* (Nov. 18, 2013), available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.

[9] *Source Code Policy*, *supra* n. 2, at 1, lines 5-6, 30-31.

[10] *Id.* at 4, lines 118-122; appendix B.

[11] The Policy uses the term COTS to include commercial item solutions. *See id.* at 1, n. 2.

solutions equally and on a level playing field."[12] If one or more COTS solutions exist, the agency shall select the solution that best meets the agency's needs, taking into account merit-based factors such as performance, total cost of ownership, security and privacy protections, and other factors.[13]

- Third, if the agency determines that no existing Federal or COTS solution exists, it may develop or procure custom software code. If the agency procures such code, it must (a) require delivery of the underlying source code and related documentation from the developer; and (b) secure "unlimited rights" to such source code and documentation,[14] and ultimately make such code available to all other federal agencies for reuse.[15] In addition, pursuant to a proposed pilot program, each agency must release at least twenty percent of all custom code procured each year as OSS.[16]

In each of these three steps, covered agencies must, consistent with existing OMB policy, "evaluate safe and secure cloud computing options."[17] The guidance fails to indicate, however, whether agencies must apply the requirements of step 3 to available cloud solutions, and if so, how such a requirement would work in practice. Moreover, although Appendix B to the proposed Source Code Policy indicates that agencies should "[k]eep . . . in mind" existing OMB guidance requiring them to evaluate merit-based factors such as total cost of ownership, price-for-performance, and security, privacy, and interoperability in all three stages of their analysis, this requirement is not reflected in the actual text of the proposed Policy. Also, the Policy provides no guidance on how agencies are to proceed where a custom software solution that provides the best mix of performance and value is not available with unlimited rights in the underlying source code (or where the cost of procuring such rights would be significant).

It bears emphasizing that most of this guidance—such as the need to focus on total cost of ownership and other merit-based factors; the preference for using cloud-based solutions or existing federal software solutions; the need to make decisions on a technology-neutral basis—is already set forth in existing OMB memoranda. The only novel aspects of the proposed Policy are those that *restrict* Federal agencies' ability to comply with this existing guidance when procuring custom software by *mandating* that agencies select solutions for which unlimited rights in source code are available. Thus, the Policy appears to require procurement of solutions for which unlimited rights in source code are available *even if* doing so would conflict with other existing OMB guidance (*e.g.*, because the solution does not offer the best mix of performance and price, is insecure, or would impose a higher total cost of ownership).

[12] *Id.* at 4-5, lines 129-130.

[13] *Id.* at 4-5, lines 124-134 (internal citations omitted); appendix B.

[14] *Id*. at 5, lines 152-168 (internal citations omitted); appendix B.

[15] *Id.* at 6, lines 170-175.

[16] *Id*. at 8, lines 224-251 (internal citations omitted); appendix B. The proposed Policy also requires that all custom code developed by Federal employees as part of their official duties must be released as OSS. *Id*. at 8, lines 238-243.

[17] *Id.* at 4, lines 113-115; appendix B.

The requirements to secure "unlimited rights" to custom software code and to release at least twenty percent of all custom code procured each year as OSS could harm rather than advance the Federal Government's interests in the longer term.

As explained below, we believe that the proposed Source Code Policy will have many unintended consequences, including higher custom software costs. This defeats one of the proposed Source Code Policy's main purposes which is saving taxpayer dollars.

III. Specific Concerns

BSA strongly supports the freedom of Federal agencies to select the best solution available, including open-source solutions, where they offer the optimal mix of total cost of ownership, performance, security, and other factors. Indeed, several BSA members offer or support OSS solutions that may satisfy these criteria in any given tender. Applicable law and OMB guidance, however, already give Federal agencies the freedom to select such OSS solutions—and indeed effectively direct them to select such solutions where they offer the best mix of performance and value. Accordingly, we question whether the proposed Source Code Policy is necessary. We do not believe that an agency should prefer an OSS solution to a proprietary one if its total cost of use, security, and performance are inferior, in particular because such a preference would be for the purpose of allowing a hypothetical reuse of the source code.

Moreover, because the mandates set forth in the proposed Policy would have the effect of *restricting* Federal agencies' current ability to procure custom code based on merit and value, and thereby *deprive* them of their freedom to select the solution that best fits their needs, we believe the most likely effect of the proposed Policy would be to undermine the Government's efforts to achieve its other important IT policy goals. Our specific concerns in this regard are set out below.

A. Scope

We are concerned about the practical aspects of the implementation of the proposed mandate that new custom code whose development is paid for by the Federal Government should be made available for reuse across federal agencies and that a portion of that new custom code (at least twenty percent) be released to the public as OSS. This requirement may be misinterpreted and it could be inadvertently extended to software solutions developed and/or modified for Federal Government use by a contractor when a portion of the development costs are not attributed to government contracts. Solutions that are custom-developed by contractors are often based on a code-base that is either COTS or custom but pre-existing, and which is then customized to meet the requirements of the customer, e.g. to add specific features or to enable interoperability with another system. The proposed Source Code Policy should explicitly exclude such cases from its scope.

When COTS solutions are sold to Federal agencies, some amount of customization may be required so that the software can be properly installed and implemented and so that generalized software functionality can be tailored to a desired usage. This customization should not be in the scope of the proposed Source Code Policy because it will not likely be useful to multiple agencies. The utility of the customization depends on underlying architecture and specific usage to which the software is put, which are not standard across agencies. These customizations are often worked back into the underlying proprietary product and/or used for other customers in similar situations.

Unfortunately, the Source Code Policy would negatively impact this very common, if not ubiquitous practice, and may limit useful development of solutions in the industry. The proposed Source Code Policy clearly states (line 138) that it applies to customizations of COTS products. Under Federal Copyright Law, the owner of an existing work owns any derivative works of the underlying copyrighted work. Any customization is a derivative work under law and thus the proposed Source Code Policy could conflict with rights granted under the Copyright Act to the developer of the underlying software, contrary to the longstanding policy of the Copyright Act.

Should the proposed Source Code Policy be implemented as currently written, it could lead to negative outcomes. *First*, Federal agencies would have to pay materially higher fees because companies with proprietary intellectual property would be asked to give up what is the near-equivalent to the ownership of those rights. *Second*, most companies would simply refrain from providing customized COTS solutions to Federal agencies preventing agencies from having access to the best-available solutions that could be available for its use.

At minimum, the proposed Source Code policy should redefine “custom code” to exclude anything that is a derivative work of a vendor’s existing proprietary work.

B. <u>Security</u>

Given recent high-profile cyber-security attacks by malicious actors against enterprise IT systems—including successful attacks against Federal IT systems[18]—it is more apparent than ever that security must be a top priority for Federal agencies when procuring and implementing IT solutions. This is particularly true for Federal IT systems that handle personal data or other sensitive information.

BSA and its members applaud recent efforts by OMB and other Federal authorities to strengthen the security and resilience of Federal IT systems. Given the rapidly increasing sophistication and capabilities of cyber-criminals and other adversaries, it is essential that Federal agencies have the ability—and indeed the duty—to procure IT solutions that effectively protect Federal IT systems against data theft or other malicious intrusions. As drafted, however, the proposed Source Code Policy would undermine Federal efforts to strengthen IT security. The proposed Source Code Policy appears to require agencies to procure custom software solutions for which the source code is available even if the agency identifies a competing solution (for which source code is not available) that is more secure and that offers the same or better mix of performance and value.[19] In short, Federal agencies are likely to read the proposed Source Code Policy to require them to place a higher premium on the availability of unlimited rights in custom software source code than in the overall security of the software.

[18] *See, e.g.*, Cyrus Farivar, *Federal agency hit by Chinese hackers, around 4 million employees affected*, ARS TECHNICA (June 4, 2015), available at http://arstechnica.com/security/2015/06/federal-agency-hit-by-chinese-hackers-around-4-million-employees-affected/.

[19] As noted, Appendix B to the proposed Policy states that federal agencies must “[k]eep . . . in mind” security as one of several factors in all three steps of their analysis. This formulation is ambiguous, and agencies are unlikely to interpret it as requiring them to procure more-secure custom software even where unlimited rights in source code are unavailable. Moreover, this aspect of Appendix B is not reflected in the text of the proposed Policy itself.

The proposed Source Code Policy appears to take the view that securing unlimited rights in source code, and making such code available for public review, will necessarily make such software secure because communities will develop around the source code to identify and fix any security vulnerabilities that might exist.[20] This view, however, rests on a critical assumption—namely, that active and engaged communities will invariably arise around any software code that Federal agencies publish, and that this community will have the expertise and incentive to identify and fix security vulnerabilities in the code.

There are good reasons, however, to question whether this assumption will hold true in all or even most cases of published Federal custom code. A Federal agency may procure custom software under the Policy only if no appropriate Federal or COTS solution already exists. This suggests that the agency's requirements subject to the Policy often will be quite unique, since broader market demand for such software would likely have already resulted in existing Federal or COTS solutions. But it is precisely such unique, one-off software programs that are likely to be of least interest to large, sophisticated communities of open-source developers who would be willing to invest the time and energy needed to review the code effectively and continuously for security vulnerabilities.

The fact is that reviewing software code for security vulnerabilities is a complex and time-intensive task which requires a high degree of expertise. It is unrealistic to expect that every single line of code published by Federal agencies pursuant to the Policy will be scrutinized carefully by developers with the experience and expertise needed to identify and fix potential vulnerabilities, especially if such developers perceive that the program is unlikely to be used by a broad audience of users. Malicious hackers, by contrast, would have strong incentives to scour such Federal source code for vulnerabilities, particularly if they believe that they can exploit such vulnerabilities before they are identified and fixed. Accordingly, there is a real risk that implementation of the proposed Source Code Policy, as drafted, would increase the vulnerability of Federal IT systems to security attacks.

We appreciate that the proposed Source Code Policy sets forth an exception in cases where release of source code "would create an identifiable risk to the stability, security, or integrity of the agency's systems or personnel."[21] This exception, however, is inadequate for the following reasons:

- *First*, by requiring Federal agencies to establish that release of source code "would" create an "identifiable" security risk, the Proposal places an unreasonably high evidentiary burden on agencies wishing to avail themselves of the exception. Given the overriding importance of ensuring that agencies adequately protect the security of Federal IT systems, Federal CIOs should be excused from the Policy's strictures so long as they have a reasonable belief that the release of source code could result in a material risk to security. The proposed security exception should also expressly include situations in which the agency has reasonable doubts that communities with the necessary security expertise will actively engage to identify and fix security vulnerabilities in the code. Similarly, the final policy should not include the statement that "OMB expects exceptions to be rare,"[22] since OMB cannot predict at this stage how often Federal agencies may

[20] *See, e.g.*, *Source Code Policy*, *supra* n. 2, at 6, lines 184-189.

[21] *See Source Code Policy*, *supra* n. 2, at 12, lines 409-410.

[22] *Id.* at 12, line 414

need to invoke this exception to protect the security of federal IT systems, and this statement could improperly dissuade agencies from legitimately relying on the exception.

- *Second*, even with these changes, the proposed Policy is not sufficiently clear in directing Federal agencies to place a higher priority on security in their procurement of custom software solutions than on the ability to obtain unlimited rights in source code. The final Policy should be explicit and unambiguous in directing Federal agencies to select the most secure custom software solution available (all other things being equal), even if the vendor of such solution is unwilling to provide unlimited rights in the source code to such software. In addition, when open source software is used, the Policy should direct Federal agencies to retain experts in the use and maintenance of open source software to avoid security and downtime risks.

C. Technology Neutrality, Performance, and Value

Under existing federal law and policy, Federal agencies must adopt a technology-neutral approach when procuring IT products and services and must evaluate competing options on their merits, including total cost of ownership.[23] BSA strongly supports this policy. It has enabled the Federal Government to achieve higher levels of cost-efficiency while giving federal agencies the freedom to obtain IT solutions that best suit their needs at the best prices. The policy has also spurred greater participation and competition in the federal IT procurement market, which likewise has helped drive down costs and increase choices.

We are encouraged that the proposed Source Code Policy acknowledges the importance of the technology neutrality principle in general. It appears, however, that the Policy abandons this principle with regard to the procurement of custom software. Rather than directing Federal agencies to utilize merit-based evaluation processes that focus on performance and value, the Policy requires agencies to procure only those custom software solutions for which unlimited rights in source code are available. In an era of rapidly increasing Federal IT demands and limited IT budgets, this is precisely the wrong message that agencies should be following.

We are particularly concerned that this policy could detract from existing Federal policy requiring agencies to select cloud-based solutions where available. Given the tremendous potential efficiency, performance, and flexibility advantages that cloud-based solutions may provide to the Federal Government as compared to traditional software offerings, it would be deeply contrary to the Government's interests if Federal agencies were to interpret the Policy as directing them away from cloud-based solutions and towards traditional software offerings, merely because the latter could be viewed as providing a better chance to demand unlimited rights in source code. We also have concerns that agencies, in order to satisfy the Policy's "twenty percent OSS" requirement, might seek out traditional custom software solutions even where they could obtain the functionality they need more efficiently as a cloud-based service.

As the proposed Policy notes, many companies—including many BSA members—develop, distribute, and support software under OSS licenses (as well as under proprietary and mixed-source licenses) because this is what their customers want and what the market demands in certain circumstances. Their development and licensing decisions are not dictated by a pro- or anti-OSS bias, but motivated and informed by the realities of the market. Most Federal agencies today run many different software programs from many different vendors, and these programs are distributed under a wide array of licenses. To ensure that Federal agencies can continue to procure software efficiently, and to integrate any custom software they

[23] *See, e.g.*, OMB, *Memorandum on Technology Neutrality*, *supra* n. 7.

purchase into their existing IT systems in a secure and cost-effective way, they must have the freedom to select whatever delivery and licensing model best suits their particular needs in any given case.

The proposed Source Code Policy would deprive Federal agencies of this freedom. It would almost certainly reduce the choices available to Federal agencies, since not all software vendors will be willing to offer unlimited rights in their source code. The Policy also would likely result in higher prices, since vendors may insist on being compensated for providing unlimited rights in their source code—including for the lost opportunity costs of not being able to charge future customers for licenses to such software (since any potential future customer could simply download the source code for free from the Federal government repository). The Policy may have a particularly detrimental impact on smaller government contractors, who may have less experience in working with and fostering active open-source communities around software, and who might be less able to accept the economic trade-offs that would be required of them in abandoning any future rights to monetize their custom-developed software.

Although the Policy appears to assume that any such additional costs for software will be effectively recouped by the fact that other Federal agencies can reuse such software free of charge,[24] the Policy does not empower Federal agencies to evaluate these potential trade-offs in any individual case. Instead, it requires them to pay for unlimited rights in source code even if they have strong reasons to believe that few if any other users will ever have an interest in the source code. This is problematic, since the very fact that such software is not already available in the marketplace—and therefore must be developed on a customized basis—suggests that there may be little or no market demand for such software. In those cases, the potential benefits of sharing the source code, and the potential cost savings to the Government of doing so, might be small to non-existent, while the added upfront cost for the first acquiring agency are likely if not certain.

In addition, it is also important to point out that it may be extremely difficult - and even impossible in many cases - to determine what twenty percent of a program that includes millions of lines of code would be. Furthermore, the costs associated with making this determination would be very high.

To address these problems, the proposed Source Code Policy should be revised to remove the requirement that twenty percent of custom code shall be released each year as OSS and to explicitly reaffirm that Federal agency IT procurement should be "built around the use of merit-based requirements, development and evaluations processes that promote procurement choices based on performance and value."[25] Federal agencies also should be authorized to seek unlimited rights in source code for any custom-developed software they procure only if doing so would not result in the agency selecting an option with a lower overall performance-to-value ratio.

D. <u>Standards</u>

Critical to the Federal Government's overall IT acquisition strategy is to ensure that when acquiring IT systems and services, Federal agencies seek out functionality, outcomes and capabilities to maximize competition and innovation, rather than defaulting to one proscriptive

[24] *See, e.g.*, *Source Code Policy*, *supra* n. 2, at 7, lines 220-222.

[25] OMB, *Memorandum on Technology Neutrality*, *supra* n. 7.

development process or another. The use and adoption of standards that are global, voluntary, and developed through industry-led multi-stakeholder processes reduces costs, increases competition, promotes innovation, facilitates interoperability and provides a greater return on investment.

Given the heterogeneous mix of enterprise IT systems today, interoperability—the ability of products and services to exchange and use data—is of particular importance. One effective approach to interoperability is to focus on technology standards, and all leading CIOs today place a priority on evaluating which standards will best promote interoperability within their IT systems. Whether a software program implements key standards and thereby supports interoperability, however, has no relation to whether it is licensed as open source. Likewise, a policy mandating the use of OSS offers no greater guarantee of interoperability than one mandating the use of proprietary software.

Rather, the focus for Federal agencies should be on technology standards that facilitate interoperability and data exchange with other government agencies and with the citizens they serve. A policy that requires agencies to purchase OSS may in fact limit their ability to select products that implement key standards or otherwise facilitate interoperability—thereby increasing complexity and depriving both governments and citizens of the benefits of more open and participatory government. This would run directly counter to the core objectives of the Administration's *Second Open Government National Action Plan*, which this proposed Source Code Policy is required to support.[26]

E. Community Support

As the proposed Source Code Policy recognizes, making source code broadly available can have important benefits in those cases where a community of developers emerges that is invested in improving the code, maintaining it, and driving it forward. As the Policy acknowledges, "[m]aking code available with an OSS license can enable continual improvement of Federal code projects *when a broader community of users implements the code for its own purposes and publishes bugs and improvements*."[27] For this reason, "[c]ommunities are critically important to the long term viability of open source projects."[28] What the proposed Policy fails to appreciate is the challenges that may arise in generating an active and engaged community around any particular open source code project, especially in cases where an agency requires a custom software solution—and the potential downsides to the Federal Government in those cases where a such a community fails to emerge.

Active and engaged communities typically emerge around open-source software projects only where participants perceive that the project addresses an important market demand, and therefore that any time and resources they invest in improving the software will have significant, real-world benefits. Even a cursory glance at the thousands of projects in leading open-source repositories that have been abandoned by users (and even at times by the original developer) demonstrates the importance—and challenges—of strong and active community support to the viability of open-source software projects.

[26] Source Code Policy, supra n. 2, at 2, lines 43-44.

[27] *Id.* at 2, lines 35-38 (emphasis added).

[28] *Id.* at 8, line 254.

The proposed Policy assumes that such communities will naturally arise around source code packages published by Federal agencies pursuant to the Policy. But that assumption is unfounded. The fact that the agency cannot meet its software needs through existing Federal and COTS solutions is likely in many cases to reflect *the lack* of market demand for such software. In those cases, there are good reasons to be skeptical that an active and engaged community of developers will emerge to maintain and improve the code. Furthermore, most Federal agencies are unlikely to have the time, resources, or expertise to generate community interest in the code themselves, particularly over the many years that the agency (presumably) intends to use the software. Thus, in many cases, the perceived benefits to the Federal Government of publishing source code for custom-developed software may never materialize.

Publishing source code for which little or no community support emerges, by contrast, could have important negative repercussions for Federal agencies. First and foremost is the risk, described in Section III.B of these comments, that malicious actors may use access to the source code to identify and exploit vulnerabilities in the software. To guard against this risk, agencies would need to hire third-party experts to undertake a comprehensive security audit of the source code, and update that audit every time the code is updated, which will add to total cost of the solution. In addition, agencies may end up paying significant premiums for unlimited rights in source code, but be unable to realize the benefits of such rights at a practical level where no community emerges to maintain the code and drive it forward.

As drafted, the proposed Policy does not authorize Federal agencies to weigh these competing interests in deciding whether to comply with the Policy, other than to allow agencies to "prioritize the release of custom code that [is] potentially useful to the broader community."[29] Instead, it requires agencies to obtain unlimited rights in source code, and to make such code available across the Government, for *all* custom software code they procure. In addition, the Policy's mandate that agencies release at least twenty percent of such source code under an OSS license will limit agencies' ability to take these competing concerns into account. Accordingly, there is a significant risk that the Policy as drafted could harm rather than advance the Federal Government's interests in the longer term.

* * * * *

BSA appreciates this opportunity to provide these perspective on OMB's proposed Source Code Policy. We would be happy to answer any questions the Office might have on these comments.

[29] Source Code Policy, supra n. 2, at 8, lines 232-233.