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

The U.S. Government is committed to improving the way Federal agencies buy, build, and deliver information technology (IT) and software solutions to better support cost efficiency, mission effectiveness, and the consumer experience with core Government programs. Each year, the Federal Government spends more than $9 billion on software through more than 50,000 transactions.[1] A large portion of Government software—including proprietary, open source, and mixed source options—is commercially-available "off the shelf" (COTS) software[2] that is developed and owned by either private vendors or an open source provider, requiring no additional custom code to be written for its use in the Federal Government.[3]

However, when Federal agencies are unable to identify an existing Federal or COTS software solution that satisfies their specific needs, an agency may choose to develop a custom software solution on its own or pay for its development. When agencies procure custom-developed code, they are not always in a position to make their new code broadly available for Federal Government-wide reuse.[4] In some cases, agencies may have difficulty establishing under the terms of the contract that the software was produced in the performance of a Federal Government agreement. Furthermore, even when agencies are in a position to make their code available on a Government-wide basis, they do not routinely make their source code discoverable and usable to other agencies in a consistent manner. These shortcomings can result in duplicative acquisitions for the same code and inefficient spending of taxpayer dollars. This policy seeks to address these challenges by laying out steps to help ensure that new custom-developed Federal source code be made broadly available for reuse across the Federal Government.[5] This is consistent with the *Digital Government Strategy's* "Shared Platform" approach, which enables Federal employees to work together—both within and across agencies—to reduce costs, streamline development, apply uniform standards, and ensure consistency in creating and delivering information.[6] Enhanced reuse of custom-developed code across the Federal Government can have significant benefits for American taxpayers, such as reducing Federal vendor lock-in,[7] decreasing duplicative costs for the same code, increasing transparency across the Federal Government, and minimizing the challenges associated with integrating large blocks of code from multiple sources.



---

[1] *Building on Progress: Improving the Way the Government Buys IT*, Office of Management and Budget, Executive Office of the President, December 21, 2015. https://www.whitehouse.gov/blog/2015/12/21/building-progress-improving-way-government-buys-it

[2] For purposes of this policy, the term "COTS" also generally encompasses commercial item solutions.

[3] *See* "Appendix A: Definitions" for definitions of many of the technical terms used in this section and throughout this policy.

[4] Additional contract guidance will be available through Project Open Source.

[5] Limited exceptions may apply. *See* "Exceptions" section for additional information.

[6] *Digital Government: Building A 21st Century Platform To Better Serve The American People*, Office of Management and Budget, Executive Office of the President, May 23, 2012. https://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

[7] "Vendor lock-in" refers to a situation in which the customer depends on a single supplier for a product and cannot easily move to another vendor without sustaining substantial cost or inconvenience. Vendor lock-in can potentially raise costs and reduce innovation within that service, and it can result in reduced competition on future related software acquisitions.

While the benefits of enhanced Federal code reuse are significant, additional benefits can accrue when code is also made available to the public as Open Source Software (OSS). Making 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. A number of private sector companies have already shifted some of their software development projects to an open source model,[8] in which the source code of the software is made broadly available to the public for inspection, improvement, and reuse. In fact, several Federal agencies and component organizations also have already begun publishing custom-developed code under open source licenses or in the public domain, as discussed further below. Moreover, the Administration made a commitment, as part of its *Second Open Government National Action Plan,*[9] to develop an Open Source Software policy that, together with the *U.S. Digital Services Playbook*,[10] will support improved access to custom code developed for the Federal Government. This policy fulfills that commitment in an effort to improve U.S. Government software development and make the Government more open, transparent, and accessible to the public. Just as the Administration's *Open Data Policy*[11] contributed to the creation of valuable and successful private businesses and services based upon open data released by the Government,[12] improving access to taxpayer-funded source code can help facilitate similar results predicated on OSS.



[8] For example, Microsoft has released the .NET software framework--used by millions of developers to build and operate websites and other large online applications--under an OSS license (*see* https://blogs.msdn.com/b/dotnet/archive/2014/11/12/net-core-is-open-source.aspx). Additionally, Apple Computer, Inc. made the Swift programming language--used to develop applications on Apple operating systems such as OS X and iOS--available as OSS (*see* https://developer.apple.com/swift/blog/?id=34). A third example is Google's recent decision to open source its artificial intelligence system TensorFlow, which is utilized by applications such as Google Search, Google's voice recognition application, and Google Translate (*see* https://googleblog.blogspot.com/2015/11/tensorflow-smarter-machine-learning-for.html)

[9] *The Open Government Partnership: Announcing New Open Government Initiatives as part of the Second Open Government National Action Plan for The United States of America*. September, 2014. Page 2. https://www.whitehouse.gov/sites/default/files/microsites/ostp/new_nap_commitments_report_092314.pdf

[10] The Digital Services Playbook consists of key "plays" drawn from successful practices from the private sector and Government that, if followed together, will help Government build effective digital services. It encourages agencies to "default to open" and seek contracts that specify that "software and data generated by third parties remains under [the U.S. Government's] control, and can be reused and released to the public as appropriate and in accordance with the law. It also requires an explanation "[i]f the codebase has not been released under an open source license." https://playbook.cio.gov/.

[11] *Open Data Policy-Managing Information as an Asset*. May 9, 2013. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-13.pdf

[12] *See* https://data.gov/impact for examples of Federal open data being used in various methods and industries.

## 1. Objectives

This policy will accomplish the following objectives:

1. Provide guidance to covered agencies[13] on software procurement considerations that must be made prior to acquiring any custom-developed software. This applies only to software developed in the performance of a Federal agreement;

2. Establish policy requirements for Government-wide source code receipt and reuse, including requirements for covered agencies to require delivery of source code produced in the performance of a Federal Government agreement and, subject to certain exceptions,[14] make it broadly available Government-wide;

3. Establish requirements for releasing code in the public domain or as OSS, including requirements for covered agencies to secure the rights necessary to make some custom-developed source code releasable to the public as OSS; and

4. Provide instructions and support to facilitate implementation of this policy.

## 2. Scope and Applicability

The requirements outlined in this policy apply to all covered agency agreements that (1) relate to Federally-procured software solutions; and (2) include requirements for, or may result in, custom-developed source code. Source code developed for National Security Systems, as defined in 44 U.S.C. §3542, is exempt from the requirements of this policy. For National Security Systems, agencies shall follow applicable statutes, Executive Orders, directives, and internal agency policies.

This policy does not require that existing custom-developed source code created by third party developers or vendors for the Federal Government be retroactively made available for Government-wide reuse or as OSS; however, making such code available for Government-wide reuse or as OSS, to the extent permissible under existing contracts or other agreements, is strongly encouraged. This policy also does not apply to software code whose development was not paid for by the Federal Government, even if later procured by the Federal Government (*e.g.*, Microsoft Word).

Furthermore, this policy applies to all custom code created by covered agency employees in the course of their official duties, subject to certain exceptions noted below. For such code, it is encouraged that covered agencies apply the requirements of this policy retroactively to the extent practicable.

The covered agencies' Chief Information Officers (CIO), Chief Acquisition Officers (CAO) and other key stakeholders shall immediately begin working together to implement this guidance.



[13] *See* definition of "Covered Agency" in Appendix A: Definitions.

[14] *See* "Exceptions to Government-wide Reuse or to Publication" in the Implementation section of this policy.

## 3. Software Procurement Considerations

In meeting their software needs, covered agencies should give preference to existing Federal software solutions (*e.g.*, Federal shared services or existing reusable source code) or a purchasable off-the-shelf software solutions (*e.g.*, COTS) that can efficiently and effectively meet their operational and mission needs. When a covered agency determines that these alternatives do not meet its needs, the agency may need to procure custom-developed source code built from scratch or built on top of a proprietary solution.

Consistent with OMB policy, in the course of deciding whether a custom solution is necessary, covered agencies must conduct the following three-step analysis (as illustrated in *Appendix B*). This analysis is intended to mitigate unnecessary spending on custom-developed software solutions by ensuring that existing Federal and commercial solutions, including existing proprietary and/or open source solutions and reusable code, are considered as potential alternatives. In any of the following steps, covered agencies may consider hybrid solutions (*i.e.*, those containing a mixture of existing, COTS, and/or custom solutions) if a preexisting Federal software solution or COTS solution does not—on its own—fully meet the covered agency's operational and mission needs.[15] Furthermore, consistent with OMB policy, covered agencies must evaluate safe and secure cloud computing options throughout every step of the software procurement analysis.[16] These steps are consistent with the long-standing OMB policy commonly known as "Raines' Rules."[17]

- ***Step 1 (Alternatives Analysis):*** When evaluating whether or not to procure a software solution, covered agencies must first conduct an alternatives analysis and demonstrate a preference for the use of existing software solutions for which the Government holds appropriate license rights or ability to reuse. This may include Federal shared services or previously developed code available for Government-wide reuse.

- ***Step 2 (COTS Solutions):*** If a covered agency's alternatives analysis concludes that no existing Federal solution efficiently and effectively meets its operational and mission needs, a covered agency must subsequently explore whether an appropriate COTS solution is available. Consistent with OMB's previous instructions related to Technology Neutrality,[18] as part of this process, covered agencies must conduct market research and analyze alternatives that include proprietary, open source,[19] and mixed-source software



[15] This analysis is consistent with current Federal procurement policy (*See* 48 C.F.R. §52.227-17), and the Clinger-Cohen Act of 1996 (*See Chapter 7 – Acquiring Information Technology, 40 U.S.C. Subtitle III*)
[16] *Federal Cloud Computing Strategy*. February 8, 2011.
https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf
[17] OMB Memorandum M-97-02. *Funding Information Systems Investments*.
https://www.whitehouse.gov/omb/memoranda_m97-02/
[18] *Technology Neutrality*. January 7, 2011.
https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf
[19] For purposes of Federal IT acquisitions, OSS must be considered a commercial item and be given appropriate statutory preference per 41 U.S.C. §103 (1)(B), so long as the OSS product is available for license to the general public and meets the other terms therein. When using or modifying OSS, covered agencies are strongly encouraged to consider which license is associated with the software. Licenses affect how the work can be used, modified, and how derivative works must be treated. Agencies must comply with the terms of the licensed work. Government

solutions equally and on a level playing field. Covered agencies must then select, if available, a software solution that best meets the operational and mission needs of the agency, taking into consideration factors such as performance, total life-cycle cost of ownership, security and privacy protections, interoperability, ability to share or reuse, resources required to later switch vendors, and availability of support.

- ***Step 3 (Custom Development):*** If a covered agency's alternatives analysis concludes that no existing Federal and/or COTS solutions can fully satisfy its operational and mission needs, the agency may consider custom-developed source code. This includes developing a solution from scratch, or developing a solution to customize an existing Federal or COTS product. When developing or acquiring custom code, covered agencies must comply with the policy requirements outlined below.

## 4. Government-Wide Code Reuse

Under U.S. copyright law, all software created by Federal Government employees as a "government work" is in the public domain and, accordingly, is not subject to copyright protection in the United States.[20] However, software created on behalf of the Government by third parties, such as private sector vendors, is subject to copyright protection. Currently, the majority of software solutions used in the Federal Government are developed by third parties.

As discussed earlier, the reuse of custom-developed source code purchased by the Federal Government has numerous benefits for American taxpayers. To take advantage of these benefits, all covered agencies and component organizations that procure custom-developed software solutions for the Federal Government must, at a minimum, comply with the following requirements:

(1) Require delivery of the underlying custom source code, associated documentation, and related files—from the third-party developer or vendor to the Federal organization (including build instructions and, when applicable, software user guides, other associated documentation, and automated test suites); and

(2) Secure unlimited rights to the custom source code, associated documentation, and related files—which includes the rights to reproduction, reuse, and distribution of the custom source code, associated documentation, and related files across the Federal Government.

Covered agencies that enter into agreements for the development of software should require unlimited data rights in accordance with this policy. Additional guidance, including sample language for agreements, shall be provided as a part of Project Open Source.[21]



employees and their covered agencies are encouraged to improve the OSS they use and push those fixes to the appropriate code repository. This practice benefits all users of the software because those changes can be distributed widely. This work must follow the terms of the license of the original work. For further guidance, covered agencies should look to Project Open Source at https://project-open-source.cio.gov.

[20] Per 17 U.S.C. §105, U.S. Government Works are not subject to domestic copyright protection.

[21] Additional information about Project Open Source can be found in Section 6: Implementation.

Securing Federal Government-wide reuse rights for custom code is a critical first step in gaining efficiencies in Federal software purchasing; however, without broad and consistent dissemination of the code across the Federal Government, these efficiencies cannot be fully realized. Therefore, in addition to securing the rights discussed above, covered agencies must make custom-developed code available to all other Federal agencies.[22] The "Implementation" section of this policy provides additional guidance on this requirement.

Note 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[23] and should therefore not be mislabeled as such.

## 5. Federally Funded Custom Code as Open Source Software

As previously mentioned, a number of private sector companies have shifted some of their software use and development to an open source model.[24] Similarly, when properly implemented and documented, releasing code as open source can benefit Federal agencies by allowing professional communities of practice to develop around software libraries and Application Programming Interfaces (APIs). This collaborative atmosphere makes it easier to conduct software peer review and security testing, to reuse existing solutions, and to share technical knowledge.[25] In fact, the Federal Government and partner organizations have recently begun using more OSS and publishing some of their custom software code under open source licenses or in the public domain. Some examples include:

- "We the People" [26] – This is a White House service that allows the American people to easily and interactively petition their Government. The source code for this website is freely available as OSS;[27]



[22] Limited exceptions may apply. *See* "Exceptions" section for additional information.

[23] As of the publication date of this policy, the most widely-recognized definition of "Open Source Software" – both in the U.S. and internationally – is provided by the Open Source Initiative, and provides 10 criteria that software must meet to be considered open source. This definition is accessible at https://opensource.org/osd.

[24] For example, Microsoft has released the .NET software framework -- used by millions of developers to build and operate websites and other large online applications -- under an OSS license (*see* http://blogs.msdn.com/b/dotnet/archive/2014/11/12/net-core-is-open-source.aspx). Additionally, Apple Computer, Inc. made the Swift programming language -- used to develop applications on Apple operating systems such as OS X and iOS -- available as OSS (*see* https://developer.apple.com/swift/blog/?id=34). A third example is Google's recent decision to open source its artificial intelligence system TensorFlow, which is utilized by applications such as Google search, Google's voice recognition app, and Google Translate (*see* https://googleblog.blogspot.com/2015/11/tensorflow-smarter-machine-learning-for.html).

[25] Department of Defense Chief Information Officer. *Clarifying Guidance Regarding Open Source Software (OSS).* October 16, 2009. "The continuous and broad peer-review enabled by publicly available source code supports software reliability and security efforts through the identification and elimination of defects that might otherwise go unrecognized by a more limited core development team." http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf

[26] *See:* https://petitions.whitehouse.gov/

[27] Source code available at: https://github.com/WhiteHouse/petitions

- The General Services Administration's (GSA) 18F[28] and the Consumer Financial Protection Bureau (CFPB)[29] – Both of these government organizations have policies that establish a default position to publicly publish all custom code developed by or for the organization—whether developed in-house by Federal staff or through negotiated agreements—with limited exceptions;

- The Department of Defense (DoD) – This government agency issued guidance[30] dating back to 2009 that, among other things, clarifies the use of OSS at DoD and makes clear that OSS products are on equal footing with their proprietary counterparts in terms of procurement and usage; and

- The Open Source Electronic Health Record Alliance (OSEHRA) – This is an independent 501(c)(6) organization that was established in 2011 to support the Veterans Information Systems and Technology Architecture (VistA) electronic health record system developed by the U.S. Department of Veterans Affairs. OSEHRA supports the VistA community through activities such as maintaining code repositories, providing certifications and standards, and facilitating developer engagement. The code is released under a standard OSS license.[31]

As outlined in the OMB *Open Government Directive*,[32] the three principles of transparency, participation, and collaboration form the cornerstone of an open government. Federally released OSS embodies these principles. Leveraging the skills and knowledge of individuals across the Federal Government and beyond can result in, among other things, enhancements to code quality and security as a result of public scrutiny of open source code.[33] Federal OSS can also contribute to economic growth and innovation as state and local governments, private sector companies, taxpayers, and others can reuse that code to develop products and services for the public.[34]



[28] 18F (https://18f.gsa.gov/) is a digital services delivery team within the General Services Administration (GSA). The 18F Open Source Policy is described at https://18f.gsa.gov/2014/07/29/18f-an-open-source-team/ and can be accessed at https://github.com/18F/open-source-policy/blob/master/policy.md.

[29] CFPB's source code policy is described at http://www.consumerfinance.gov/blog/the-cfpbs-source-code-policy-open-and-shared/ and can be accessed at https://cfpb.github.io/source-code-policy/.

[30] Department of Defense Chief Information Officer. *Clarifying Guidance Regarding Open Source Software (OSS).* October 16, 2009. http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/2009OSS.pdf

[31] Licensing is managed under the Apache License Version 2.0, which requires the preservation of any previous patent, copyright, and licensure language in derivative works. For more information, *see*: http://www.osehra.org/

[32] Office of Management and Budget. *Open Government Directive*. https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf

[33] The Department of Defense's OSS FAQ states that "continuous and broad peer-review, enabled by publicly available source code, improves software reliability and security through the identification and elimination of defects that might otherwise go unrecognized". *Frequently Asked Questions regarding Open Source Software (OSS) and the Department of Defense (DoD)*, https://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx.

[34] For example, 18F and the U.S. Digital Service (USDS) jointly developed https://analytics.usa.gov to provide a window into how people are interacting with the Federal Government online and made the source code available in the public domain (*see* https://github.com/18F/analytics-reporter). The cities of Philadelphia, PA (http://analytics.phila.gov/) and Boulder, CO (https://bouldercolorado.gov/stats) were able to reuse the code to provide their own citizens with real-time information on how city government websites are serving citizens.

### 5.1 Pilot Program

In furtherance of the objectives outlined in the Open Government Directive, this policy requires that covered agencies participate in the following pilot program to encourage the development and publication of custom-developed Government code as OSS.

Each covered agency shall release at least 20 percent of its newly-developed custom code each year as OSS. Custom code is defined as code for all custom software projects, modules, and add-ons that are self-contained.[35] When deciding which custom code projects to release, each covered agency should prioritize the release of custom code that it considers potentially useful to the broader community.[36]

Although the minimum requirement for OSS release is 20 percent of custom code, covered agencies are strongly encouraged to publish as much custom-developed code as possible to further the Federal Government's commitment to transparency, participation, and collaboration. Please note that this requirement refers to new code that is developed by *third party* developers or vendors on behalf of a covered agency, as opposed to code developed by Federal employees as part of their official duties. As noted previously, all new custom code developed by covered agency employees as part of their official duties shall be released to the public—subject to certain exceptions—as enumerated in Section 6 ("Exceptions to Government-wide Reuse or to Publication").

Within 120 days of the publication of this policy, OMB shall develop metrics to assess the impact of the pilot program. No later than two years after the publication date of this policy, OMB shall consider whether to issue a subsequent policy to continue, modify, eliminate, or expand the pilot program. Unless extended by OMB through the issuance of further guidance, the pilot program will expire three years (36 months) after the publication date of this policy. Please refer to the "Implementation" section of this policy for additional guidance on how to comply with the requirements of the pilot program.

### 5.2 Membership in the Open Source Community

Communities are critically important to the long term viability of open source projects. Consistent with the *Digital Government Strategy*'s principles to participate in open source communities and leverage public crowdsourcing, covered agencies should develop and release code in a manner that (1) fosters communities around shared challenges; (2) optimizes the ability of the community to provide feedback on, and make contributions to, the code; and (3) encourages Federal employees and contractors to contribute back to the broader OSS community by making contributions to existing open source projects. In furtherance of this strategy, covered agencies must comply with the following principles:

a. Leveraging Existing Communities – Whenever possible, custom code released to the public as OSS should be incorporated into existing communities of practice that are self-sustaining. For example, there are already existing communities for electronic health

[35] The definition of "custom code" can be found in Appendix A.

[36] The pilot program applies to custom code written by third party developers or vendors in the performance of a Federal agreement.

records and geospatial software.[37] Government agencies should only develop their own communities when existing communities do not satisfy their needs.

b. Open Development – Software that is custom-developed for or by covered agencies should, to the extent possible and appropriate, be developed in the open. Open development practices provide an environment in which open source code can flourish and repurposed. This principle, as well as the principle for "Releasing Code" below, shall include the distribution of a minimum viable product as open source code, engaging the public before official release,[38] and drawing upon the public's knowledge for bug fixes, algorithmic optimization, and other improvements to the project.

c. Incremental Release – In instances where software cannot be developed in the open, but is otherwise appropriate for release to the public, covered agencies must develop and use an incremental release schedule and undertake all necessary steps to make the code and associated documentation available for public use. This will assist in discouraging the practice of releasing large, bulk pieces of software code, which negates many of the positive attributes of open source software.

d. User Engagement – Like in the Administration's Open Data Policy, covered agencies must create a process to engage in two-way communication with users to solicit help in prioritizing the release of code and feedback on the agencies' engagement with the community. *See* Project Open Source for best practices and tools that can be used to implement user engagement efforts.

e. Code Contributions – One of the most powerful potential benefits of OSS lies within the communities that grow around OSS projects, whereby any party can contribute new code, modify existing code, or make other suggestions to improve the software. Communities can be used to monitor changes to code, track potential errors and flaws in code, and other related activities. These kinds of contributions should be anticipated and, where appropriate, considered for integration into custom-developed Government software or associated materials.

f. Documentation – It is important to provide OSS users and contributors with adequate documentation of source code in an effort to facilitate use and adoption. At a minimum, OSS repositories must include a README (or similar) file that includes the following information (note that additional guidance on repositories can be found in the "Implementation" section of this policy):
   i. The status of the software (*e.g.*, prototype, alpha, beta, release, etc.);
   ii. The intended purpose of the software;
   iii. Expected engagement level (*i.e.*, how frequently the community can expect to be engaged by the agency);
   iv. License details; and
   v. Any other relevant technical details on how to build, make, install, or use the software, including library dependencies (if applicable).



[37] *See* the reference to OSEHRA above for electronic health records; additionally, *see* "The Open Source Geospatial Foundation" at http://www.osgeo.org/.

[38] For the purposes of this policy, an "official release" is a release that is not in the alpha or beta test phases, and in the field of computer programming, would be designated with a version number 1.0.

# 6. Implementation

## Roles and Responsibilities

The Federal Information Technology Acquisitions Reform Act (FITARA)[39] creates clear responsibilities for agency CIOs related to IT investments and planning as well as requiring that agency CIOs be involved in the IT acquisition process. OMB's FITARA implementation guidance—M-15-14: Management and Oversight of Federal Information Technology[40]—established a "common baseline" for roles, responsibilities, and authorities of the agency CIO and the roles of other applicable Senior Agency Officials[41] in managing IT as a strategic resource. Accordingly, the heads of covered agencies must ensure that CIOs are positioned with the responsibility and authority necessary to implement the requirements of this policy in coordination with other Senior Agency Officials. As appropriate, the CIO should also work with the agency's public affairs staff, open government staff, web manager or digital strategist, program owners and other leadership, to properly identify, publish, and work with communities concerning their open source software projects.

## Project Open Source

Within 90 days of the publication date of this policy, the Administration will launch Project Open Source,[42] an online repository of tools, best practices, and schemas to help covered agencies implement this guidance. Project Open Source will be accessible at https://project-open-source.cio.gov. Project Open Source will evolve over time as a community resource to facilitate the adoption of good custom source code development and release practices. Guidance and language on open source licenses will be provided as part of Project Open Source. The repository will include further definitions, evaluation metrics, checklists, case studies, model contract language and more, and will enable collaboration across the Federal Government in partnership with the public.

## Code Repositories

Accessible repositories for the storage, discussion, and modification of custom code are a critical portion of both the Government-wide reuse and OSS pilot program portions of this policy. Covered agencies should utilize existing code repositories and common third-party repository platforms as necessary to comply with this policy. [43] Project Open Source will contain additional guidance on using custom code repositories as related to achieving the objectives of this policy.



[39] *See P.L 113-291, Subtitle D(* https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148)
[40] *See* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf
[41] Senior Agency Officials include positions that may include the Chief Acquisition Officer, Chief Operating Officer, Chief Financial Officer, Chief Acquisitions Officer, Chief Technology Officer, Chief Data Officer, Senior Agency Official for Privacy, Chief Information Security Officer, and Program Manager.
[42] Project Open Source will be modeled off of the successful Project Open Data platform that facilitates implementation of the Open Data Policy. *See* https://project-open-data.cio.gov/.
[43] Covered agencies should ensure access to these services. *See* OMB Memorandum M-10-23 (*Guidance for Agency Use of Third-Party Websites and Applications*).

## Code Inventories and Discovery

Code inventories are a means of discovering information such as the functionality and location of potentially reusable or releasable custom code repositories. Within 90 days of the publication date of this policy, each covered agency must update, and thereafter keep up to date, its inventory of agency information resources (as required by OMB Circular A-130)[44] to include an enterprise code inventory that lists all custom code developed for or by the agency after the publication date of this policy. The enterprise code inventory is not intended to house the custom code itself; rather, it is intended to serve as a tool for discovering custom code that may be available for Government-wide reuse or as OSS, and to provide transparency into custom software code that is developed using Federal funds. The inventory will indicate whether the code is available for Federal reuse, is available publicly as OSS, or cannot be made available due to a specific exception from this policy.

Covered agencies must describe projects within the inventory using extensible metadata that will be described in an inventory schema on Project Open Source. OMB will provide this inventory schema to covered agencies within 60 days of the publication date of this policy. Within 120 days of the publication of this policy, OMB will identify a suitable central location to make the reported OSS searchable and discoverable for agencies and the public. Please refer to Project Open Source for best practices, tools, and schema to implement the enterprise code inventory and harvestable files.

## Updated TechFAR Guidance

OMB's Office of Federal Procurement Policy (OFPP) and the U.S. Digital Service (USDS) will update the TechFAR Handbook[45] to highlight how agencies can go about securing Federal reuse rights and open source licenses as part of their acquisitions processes.

## Agency Policy

Within 90 days of the publication date of this policy, each covered agency CIO must develop an agency-wide policy that addresses the requirements of this memo. In accordance with OMB guidance,[46] these policies will be posted publicly. Moreover, within 90 days of the publication date of this policy, each covered agency's CIO office must work to correct or amend any policies that are inconsistent with the requirements of this memo, including the correction of policies that automatically treat OSS as noncommercial software.



[44] *See* OMB Circular A-130, Transmittal Memorandum No. 4, section 8(b)(2)(a).

[45] *See* https://playbook.cio.gov/techfar/

[46] *See* M-15-14 at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf (requiring that IT policies be posted publicly at *https://[agency].gov/digitalstrategy*, and included as a downloadable dataset in the agency's Public Data Listing).

## Accountability Mechanisms

Progress on agency implementation of the actions required in this policy will be primarily assessed by OMB through analysis of each covered agency's internal Government repositories, public OSS repositories, and code inventories, as well as data obtained through the quarterly Integrated Data Collection (IDC), quarterly PortfolioStat sessions, the IT Dashboard, and additional mechanisms to be provided via Project Open Source.[47]

## Exceptions to Government-wide Reuse or to Publication

The exceptions provided below may be applied, in specific instances, to exempt a covered agency from (1) sharing custom code with other Government agencies, or (2) publically releasing custom code that is developed by covered agency employees. Any exceptions used must be approved and documented by the agency's CIO. Please note that the exceptions below do not exempt a covered agency from acquiring unlimited data rights in newly procured custom code. Moreover, these exceptions do not apply in calculating a covered agency's codebase for purposes of the OSS pilot program; but covered agencies should, as part of their internal 20 percent of custom code selection process, refrain from selecting code that would fit any of the characteristics listed below. In the event that a covered agency's CIO believes that the agency cannot meet the 20 percent requirement of the OSS pilot program because the agency is otherwise prohibited from releasing more than 80 percent of its code, the CIO should consult with OMB.

Applicable exceptions are as follows:

1. The release of the item is restricted by another statute or regulation, such as the Export Administration Regulations, the International Traffic in Arms Regulation, or the laws and regulations governing classified information;
2. The release of the item would compromise national security, confidentiality, or individual privacy;
3. The release of the item would create an identifiable risk to the stability, security, or integrity of the agency's systems or personnel;
4. The release of the item would compromise agency mission, programs, or operations; or
5. The CIO believes it is in the national interest to exempt publicly releasing the work.

OMB expects exceptions to be rare and the result of a significant Government interest. Excepted software must still be listed in the agency's enterprise code inventory, with certain redactions allowed. Please refer to Project Open Source for additional guidance on this topic.

This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



[47] *See* https://itdashboard.gov/

## Appendix A: Definitions

**Code Contributions**: Source code or other materials written by external parties and submitted to the developers/maintainers of a software project. Some common examples of code contributions are bug fixes, new or improved features, and documentation improvements.

**Covered Agency:** For purposes of this policy, a covered agency is one that meets the definition of agency under the Federal Information Security Management Act of 2002 (FISMA). *See* 44 U.S.C. §3502.

**Custom Code:** 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.

**Derivative Works**: For the purposes of this policy, a "derivative work" is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a "derivative work".[48]

**Mixed Source**: A mixed source software solution may incorporate public domain, open source, and/or proprietary code. Developers and users of mixed source software solutions must take component-level intellectual property rights into consideration whenever modifying, reusing, or distributing source code.

**Open Development**: Open development in the framework of computer software design is a process by which developers ensure the highest possible levels of transparency, legibility, testability, and modularity in their code from the start. This process is designed to maximize the potential benefit of open sourcing that code in an incremental and agile manner, engaging the public in the development process. Open development provides a larger base for quality assurance and product support in the initial phases of a project, in addition to making code easier to read, understand, repurpose, and incorporate for other programmers who may not be able to contact the original coder for support.

**Open Source License**: OSS is often associated with a license that details the terms and conditions governing the intellectual property rights of the software and its associated source code. These licenses specify how a particular work may be reproduced, modified, or used as a component of a larger system or as a standalone piece of software.[49]



[48] *See* http://www.copyright.gov/circs/circ14.pdf

[49] As of the publication date of this policy, a valid open source license is one that is approved by the Open Source Initiative (https://opensource.org/licenses). Further licensing considerations, including suggested licenses, will be provided via Project Open Source.

**Open Source Software (OSS)**: Software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. OSS is often distributed under licenses that comply with the definition of "Open Source" provided by the Open Source Initiative (https://opensource.org/osd).[50]

**Proprietary Software**: Software with intellectual property rights that are retained exclusively by an individual or a company. Although OSS intellectual property rights can also be retained by an individual or a company (through the use of a proper OSS license), the term "proprietary software" refers to software that is typically subject to more disclosure restrictions than that which is released as open source or in the public domain. Proprietary software is typically considered to be "closed-source," in that its source code is not made broadly available to users or the general public without restrictions defined by the owner.

**Project Open Source**: An online repository of tools, guides, and best practices specifically designed to help covered agencies implement the framework presented in this policy. Project Open Source can be accessed at https://project-open-source.cio.gov. Project Open Source will evolve over time as a community resource to facilitate the effective adoption of OSS. Agencies can visit Project Open Source for a more comprehensive glossary of terms and definitions related to OSS.

**Public Domain**: The set of works for which copyrights and related rights have expired, been relinquished, or do not apply, making the work freely available to the public for any purpose. Under U.S. copyright law, works created by Government employees within the scope of their employment are not subject to domestic copyright protections under 17 U.S.C. §105. Note that this definition is unrelated to the term "public domain" as it is used in export control regulations.

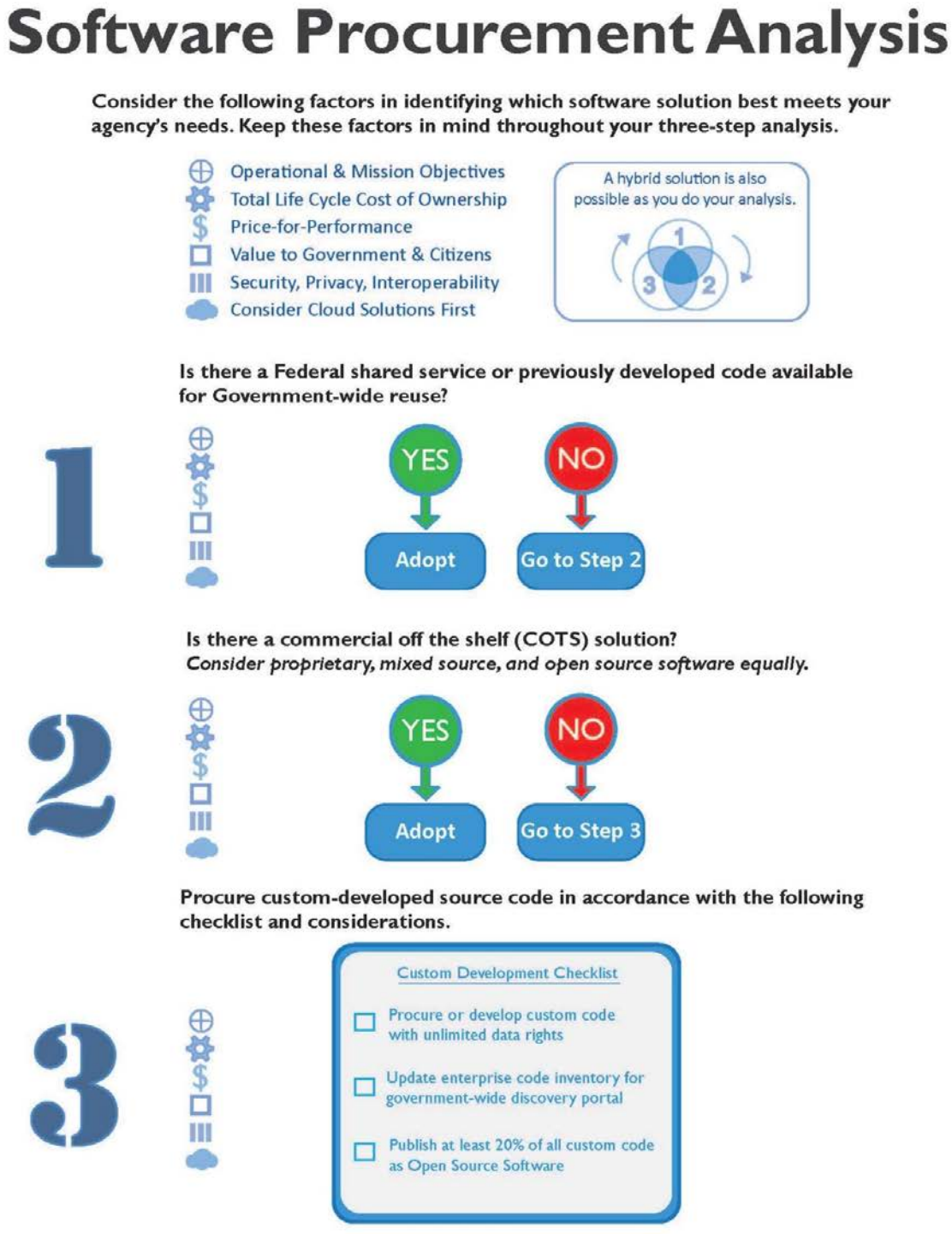
**Software**: Can refer to either: (i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; or (ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled. Software does not include computer databases or computer software documentation.[51]

**Source Code**: Information written in a computer programming language that is readable by people. Source code must be interpreted or compiled before a computer can execute the code as a program. Source code readability can benefit from the inclusion of comments or other in-code documentation that indicates the requirements and functionality of specific algorithms and other components.



[50] This definition is current as of the publication date of this policy. For future guidance regarding this definition, please refer to Project Open Source.
[51] Definition from 48 CFR §2.101

## Appendix B: Software Procurement Analysis




*This document is a supplement to the Federal Source Code Policy. It is not intended to serve as a stand-alone document.*