EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 8, 2016

M-16-21

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: **Tony Scott**
United States Chief Information Officer

Anne E. Rung
United States Chief Acquisition Officer

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 Government programs. Each year, the Federal Government spends more than $6 billion on software through more than 42,000 transactions.[1] A significant proportion of software used by the Government is comprised of either preexisting Federal solutions or commercial solutions. These solutions include proprietary, open source, and mixed source[2] code and often do not require additional custom code development.

When Federal agencies are unable to identify an existing Federal or commercial software solution that satisfies their specific needs, they may choose to develop a custom software solution on their own or pay for its development. When agencies procure custom-developed source code, however, they do not necessarily make their new code (source code or code) broadly available for Federal Government-wide reuse. Even when agencies are in a position to make their source code available on a Government-wide basis, they do not make such code available to other agencies in a consistent manner. In some cases, agencies may even have difficulty establishing that the software was produced in the performance of a Federal Government contract. These challenges may result in duplicative acquisitions for substantially similar code and an inefficient use of taxpayer dollars.

---

[1] *M-16-12: Improving the Acquisition and Management of Common Information Technology: Software Licensing.* Office of Mgmt. & Budget, Exec. Office of the President, June 2, 2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-12_1.pdf.

[2] *See* Appendix A for definitions of key technical terms used throughout this policy document.

This policy seeks to address these challenges by ensuring that new custom-developed Federal source code be made broadly available for reuse across the Federal Government.[3] 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.[4] Enhanced reuse of custom-developed code across the Federal Government can have significant benefits for American taxpayers, including decreasing duplicative costs for the same code and reducing Federal vendor lock-in.[5]

This policy also establishes a pilot program that requires agencies, when commissioning new custom software, to release at least 20 percent of new custom-developed code as Open Source Software (OSS) for three years, and collect additional data concerning new custom software to inform metrics to gauge the performance of this pilot.[6]

While the benefits of enhanced Federal custom-developed code reuse are significant, additional benefits can accrue when source code is also made available to the public as OSS. Making source code available as OSS can enable continual improvement of Federal custom-developed code projects as a result of a broader user community implementing the code for its own purposes and publishing improvements. This collaborative atmosphere can make it easier to conduct software peer review and security testing, to reuse existing solutions, and to share technical knowledge.[7] Furthermore, vendors participating in or competing for future maintenance or enhancement can do so with full knowledge of the underlying source code. A number of private sector companies have already shifted some of their software development projects to an OSS model, in which the source code of the software is made broadly available to the public for inspection, improvement, and reuse.

Several Federal agencies and component organizations have also begun publishing custom-developed code as OSS or without any restriction on use. Some of these include:

---

[3] *See* Section 6 of this policy for additional information about limited exceptions.

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

[5] "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 stifle innovation and it can result in reduced competition on future related software acquisitions.

[6] *Clinger Cohen Act of 1996*. 40 U.S.C. §§ 11301-11303.

[7] 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.

- The White House: "We the People" 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;[8]

- 18F[9] and the Consumer Financial Protection Bureau (CFPB):[10] Both of these organizations have policies that establish a default position to publish source code that is custom-developed by or for the organization. For example, both organizations contribute to the source code for the eRegulations platform,[11] a web-based interface for public viewing and commenting on proposed changes to Federal regulations. The eRegulations platform, which originated at CFPB, is being used by other Federal agencies[12] and continues to be improved based on public feedback;[13]

- The Department of Education: This agency's "College Scorecard" is a citizen-facing OSS website and accompanying application programming interface (API) that provides free tools to help potential students make informed decisions about which colleges or universities to attend;[14] and

- The Department of Defense (DOD): This agency issued a memorandum[15] in 2009 that, among other things, describes the many benefits of OSS that should be considered when conducting market research on software for DOD use.[16]

---

[8] "We the People" petitions are accessible at https://petitions.whitehouse.gov/. The source code for "We the People" is available at https://github.com/WhiteHouse/petitions.

[9] 18F (https://18f.gsa.gov/) is a digital services delivery team within the General Services Administration. 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.

[10] 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/.

[11] "eRegulations," CFPB's platform to read regulations, is accessible at http://www.consumerfinance.gov/eregulations/.

[12] The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) has adopted a beta version of "eRegulations," accessible at https://atf-eregs.18f.gov/.

[13] The publically accessible open source repository for submitting comments and proposing improvements to the "eRegulations" platform is accessible at https://github.com/eregs/notice-and-comment. 18F also developed https://analytics.usa.gov—jointly with the U.S. Digital Service—to provide a window into how people are interacting with the Federal Government online and made the source code available online (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 serve citizens.

[14] The Department of Education's College Scorecard is accessible at https://collegescorecard.ed.gov/. The open source repository for the website and API that runs the College Scorecard is available via 18F's GitHub repository, accessible at https://github.com/18F/college-choice.

[15] 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

[16] 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)*, accessible at https://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx.

The Administration made a commitment, as part of its *Second Open Government National Action Plan,*[17] to "develop an open source software policy that, together with the Digital Services Playbook, will support improved access to custom software code developed for the Federal government." [18] 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.

1. Objectives

This policy will accomplish the following objectives:

- Provide a policy to agencies[19] on considerations that must be made prior to acquiring any custom-developed code;
- Require agencies to obtain appropriate Government data rights to custom-developed code, including at a minimum, rights to Government-wide reuse and rights to modify the code. Agencies shall make such custom-developed code broadly available across the Federal Government, subject to limited exceptions;[20]
- Require agencies to consider the value of publishing custom code as OSS;
- Establish requirements for releasing custom-developed source code, including securing the rights necessary to make some custom-developed code releasable to the public as OSS under this policy's new pilot program; and
- Provide instructions and resources to facilitate implementation of this policy.

2. Scope and Applicability

The requirements outlined in this policy apply to source code that is custom-developed for the Federal Government, subject to the limited exceptions outlined in Section 6 of this document. Source code developed for National Security Systems (NSS), as defined in 40 U.S.C. § 11103, is exempt from the requirements of this policy. For NSS, agencies shall follow applicable statutes, Executive Orders, directives, and internal agency policies.

---

[17] *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.

[18] The Digital Services Playbook was developed by the U.S. Digital Service and consists of key "plays" that can help the 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/.

[19] For the purposes of this policy, an agency is one that meets the definition of executive agency under the Clinger Cohen Act of 1996. *See* Appendix A.

[20] *See* Section 6 of this policy for additional information about limited exceptions.

The policies in this document do not apply retroactively (*i.e.*, they do not require that existing custom-developed code 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 practicable, is strongly encouraged.

The agencies' Chief Information Officers (CIO), Chief Acquisition Officers (CAO), and other key stakeholders should promptly begin working together to implement this policy. Agencies are expected to issue internal policies, as necessary, to support these efforts and should expect their progress to be evaluated in accordance with accountability mechanisms described in Section 7.

3. Three-Step Software Solutions Analysis

Agencies must obtain sufficient rights to custom-developed code to fulfill both the Government-wide reuse objectives and the open source release objectives outlined in this policy's pilot program.

In meeting their software needs, agencies must conduct the three-step analysis outlined below. This analysis is intended to leverage existing solutions—consistent with principles of category management[21] and shared services[22]—and suitable commercial solutions, while mitigating duplicative spending on custom-developed software solutions. These steps are consistent with the Office of Management and Budget's (OMB) long-standing policy on investments in major information systems.[23] Moreover, consistent with OMB's memorandum on Technology Neutrality,[24] agencies must consider open source, mixed source, and proprietary software solutions equally and on a level playing field, and free of preconceived preferences based on how the technology is developed, licensed, or distributed.

- ***Step 1 (Conduct Strategic Analysis and Analyze Alternatives)*:** Each agency must conduct research and analysis prior to initiating any technology acquisition or custom code development. The strategic analysis should consider not only agency mission and operational needs, but also external public initiatives and interagency initiatives such as Cross-Agency Priority Goals. Having conducted the strategic analysis, agencies shall then conduct an alternatives analysis, evaluating whether to use an existing Federal

---

[21] *See Transforming the Marketplace: Simplifying Federal Procurement to Improve Performance, Drive Innovation, and Increase Savings*, Office of Mgmt. & Budget, Exec. Office of the President, December 4, 2014. https://www.whitehouse.gov/sites/default/files/omb/procurement/memo/simplifying-federal-procurement-to-improve-performance-drive-innovation-increase-savings.pdf.

[22] *M-16-11: Improving Administrative Functions Through Shared Services*, Office of Mgmt. & Budget, Exec. Office of the President, May 4, 2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-11.pdf.

[23] *See OMB Circular No. A-11, Appendix J – Principles of Budgeting for Capital Asset Acquisitions*, Office of Mgmt. & Budget, Exec. Office of the President, July 1, 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/app_j.pdf.

[24] *Technology Neutrality*, Office of Mgmt. & Budget, Exec. Office of the President, January 7, 2011. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/memotociostechnologyneutrality.pdf.

software solution or to acquire or develop a new software solution. The alternatives analysis shall give preference to the use of an existing Federal software solution.[25]

- ***Step 2 (Consider Existing Commercial Solutions)*:** If an agency's alternatives analysis concludes that existing Federal software solutions cannot efficiently and effectively meet the needs of the agency, the agency must explore whether its requirements can be satisfied with an appropriate commercially-available solution.[26]

- ***Step 3 (Consider Custom Development):*** If an agency's alternatives analysis concludes that an existing Federal software solution or commercial solution cannot adequately satisfy its needs, the agency may consider procuring custom-developed code in whole or in conjunction with existing Federal or commercial code. When commissioning new custom-developed software, agencies must consider the value of publishing custom code as OSS and negotiate data rights reflective of its value-consideration. Agencies must also obtain sufficient rights to fulfill this policy's objectives related to Government-wide code reuse and the open source pilot program.

Agencies must also consider several factors throughout each stage of the three-step analysis:

A. Hybrid Solutions: Solutions containing a mixture of existing Federal, commercial, and/or custom-developed solutions should be considered throughout each step of the analysis.

B. Modular Architecture: Agencies should consider modular approaches to solution architecture. As discussed in the *Digital Government Strategy*, modularity can reduce overall risk and cost while increasing interoperability and technical flexibility.

C. Cloud Computing: Consistent with OMB strategy, agencies are encouraged to evaluate safe and secure cloud computing options throughout each step of the analysis.[27]

D. Open Standards: Regardless of the specific solution selected, all software procurements and Government software development projects should consider utilizing open standards whenever practicable in order to increase the interoperability of all Government software solutions. Open standards enable software to be used by anyone at any time, and can spur innovation and growth regardless of the technology used for implementation—be it proprietary, mixed source, or OSS in nature.

E. Targeted Considerations: Agencies must select 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,

---

[25] Existing Federal software solutions are those for which appropriate rights are already held by the Government, which may include commercial or custom-developed software solutions.

[26] Preference must first be given to procurement of existing commercial solutions through best-in-class vehicles identified by category management policies.

[27] *Federal Cloud Computing Strategy*, Office of Mgmt. & Budget, Exec. Office of the President, February 8, 2011. https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

interoperability, ability to share or reuse, resources required to later switch vendors, and availability of quality support. These considerations should be taken into account during all three steps of the analysis.

4. Government-Wide Code Reuse

Ensuring Government-wide reuse rights for custom code that is developed using Federal funds has numerous benefits for American taxpayers. To realize these benefits, agencies must comply with the following requirements:

A. Secure Rights for Government Reuse and Ensure Delivery of Source Code

Agencies that enter into contracts for the custom development of software shall—at a minimum—acquire and enforce rights sufficient to enable Government-wide reuse of custom-developed code. Agencies must ensure appropriate contract administration and use of best practices to secure the full scope of the Government's rights, including—but not limited to—sharing and using the code with other Federal agencies.

Additionally, in order to ensure the ability to exercise these rights, agencies must use best practices to ensure delivery of the custom-developed code, documentation, and other associated materials from the developer throughout the development process.

B. Inventory All Custom-Developed Code and Make It Available Government-Wide

Securing adequate rights to enable Government-wide reuse of custom-developed 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, agencies shall do the following:

i. Maintain a Code Inventory: As part of their broader responsibility to maintain an up-to-date inventory of agency information resources, agencies shall make custom-developed code and related information available to all other Federal agencies[28] by creating and maintaining an enterprise code inventory that lists all new code that is custom-developed for the Federal Government; and

ii. Make Custom-Developed Code Available: Agencies shall make custom-developed code available for Government-wide reuse and make their code inventories discoverable at https://www.code.gov ("Code.gov"), pursuant to the limited exceptions outlined in Section 6 of this policy.

Agencies may refer to Section 7 of this document for additional information regarding their individual responsibilities related to implementing this policy.

[28] *See* Section 6 of this policy for additional information about limited exceptions.

5. Open Source Software

5.1 Pilot Program: Publication of Custom-Developed Code as OSS

Each agency shall release as OSS at least 20 percent of its new custom-developed code[29] each year for the term of the pilot program. As discussed above, agencies must obtain sufficient rights to custom-developed code to fulfill the open source release objectives of this policy's pilot program.

When deciding which custom-developed code projects to release, each agency should prioritize the release of custom-developed code that it considers potentially useful to the broader community. Agencies should calculate the percentage of source code released using a consistent measure—such as real or estimated lines of code, number of self-contained modules, or cost—that meets the intended objectives of this requirement. Additional information regarding how best to measure source code will be provided on Code.gov.

Although the minimum requirement for OSS release is 20 percent of custom-developed code, agencies are strongly encouraged to release as much custom-developed code as possible to further the Federal Government's commitment to transparency, participation, and collaboration.

OMB expects all agencies to satisfy the requirements of this pilot program without exception. Agencies should—as part of their selection of custom-developed code to be released as OSS—refrain from selecting code that would fall under the exceptions outlined in Section 6 of this policy. In the event that an agency's CIO believes that the agency cannot satisfy the 20 percent requirement of the OSS pilot program (*e.g.*, because releasing code as OSS would create an identifiable risk to the detriment of national security), the CIO should consult with OMB.

Unless extended or supplanted by OMB through the issuance of further policy, the pilot program under this sub-section will expire three years (36 months) after the publication date of this policy; however, the rest of the Federal Source Code Policy will remain in effect. No later than two years after the publication date of this policy, OMB shall evaluate pilot results and consider whether to allow the pilot program to expire or to issue a subsequent policy to continue, modify, or increase the minimum requirements of the pilot program.

Within 120 days of the publication date of this policy, OMB shall develop metrics to assess the impact of the pilot program. Additional information on these topics will be available on Code.gov.

5.2 Participation in the Open Source Community

When agencies release custom-developed source code as OSS to the public, they should develop and release the code in a manner that (1) fosters communities around shared challenges, (2) improves the ability of the OSS community to provide feedback on, and make contributions to, the source code, and (3) encourages Federal employees and contractors to contribute back to the

[29] The definition of "custom-developed code" can be found in Appendix A.

broader OSS community by making contributions to existing OSS projects. In furtherance of this strategy, agencies should comply with the following principles:

A. Leverage Existing Communities: Whenever possible, teams releasing custom-developed code to the public as OSS should appropriately engage and coordinate with existing communities relevant to the project. Government agencies should only develop their own communities when existing communities do not satisfy their needs.

B. Engage in Open Development: Software that is custom-developed for or by agencies should, to the extent possible and appropriate, be developed using open development practices. These practices provide an environment in which OSS can flourish and be repurposed. This principle, as well as the one below for releasing source code, include distributing a minimum viable product as OSS; engaging the public before official release;[30] and drawing upon the public's knowledge to make improvements to the project.

C. Adopt a Regular Release Schedule: In instances where software cannot be developed using open development practices, but is otherwise appropriate for release to the public, agencies should establish an incremental release schedule to make the source code and associated documentation available for public use.

D. Engage with the Community: Similar to the requirement in the Administration's *Open Data Policy*, agencies should create a process to engage in two-way communication with users and contributors to solicit help in prioritizing the release of source code and feedback on the agencies' engagement with the community.

E. Consider Code Contributions: One of the 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 throughout the software development lifecycle. Communities help 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. Agencies must ensure that their repositories include enough information to allow reuse and participation by third parties. In participating in community-maintained repositories, agencies should follow community documentation standards. At a minimum, OSS repositories maintained by agencies must include the following information:
    i. Status of software (*e.g.*, prototype, alpha, beta, release, etc.);
    ii. Intended purpose of software;
    iii. Expected engagement level (*i.e.*, how frequently the community can expect agency activity);

[30] 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 typically be designated with a version number 1.0.

iv. License details; and
v. Any other relevant technical details on how to build, make, install, or use the software, including dependencies (if applicable).

6. Exceptions to Government Code Reuse

The exceptions provided below may be applied, in specific instances, to exempt an agency from sharing custom-developed code with other Government agencies. These exceptions do not apply to the OSS pilot program.[31] Any exceptions used must be approved and documented by the agency's CIO for the purposes of ensuring effective oversight and management of information technology resources.

Applicable exceptions are as follows:

1. The sharing of the source code is restricted by law or regulation, including—but not limited to—patent or intellectual property law, the Export Asset Regulations, the International Traffic in Arms Regulation, and the Federal laws and regulations governing classified information;

2. The sharing of the source code would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy;

3. The sharing of the source code would create an identifiable risk to the stability, security, or integrity of the agency's systems or personnel;

4. The sharing of the source code would create an identifiable risk to agency mission, programs, or operations; or

5. The CIO believes it is in the national interest to exempt sharing the source code.

For excepted software, agencies must provide OMB a brief narrative justification for each exception, with redactions as appropriate.

7. Implementation

7.1 Roles and Responsibilities

The Federal Information Technology Acquisition Reform Act (FITARA)[32] 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

[31] *See* Section 5 for additional information regarding the pilot program.
[32] FITARA was codified as part of the *National Defense Authorization Act for Fiscal Year 2015* (Title VIII, Subtitle D, H.R. 3979); accessible at https://www.congress.gov/bill/113th-congress/house-bill/3979.

guidance[33] established a "common baseline" for roles, responsibilities, and authorities of the agency CIO and the roles of other applicable Senior Agency Officials[34] in managing IT as a strategic resource. Accordingly, agency heads must ensure that CIOs and Senior Agency Officials, including CAOs, are positioned with the responsibility and authority necessary to implement the requirements of this policy. As appropriate, Senior Agency Officials 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 collaborate with communities on their OSS projects.

Moreover, in support of the objectives and requirements of this policy, agencies should strengthen internal capacity to efficiently and securely deliver OSS as part of regular operations. Additional information on this topic will be provided on Code.gov.

7.2 Code Inventories and Discovery

Inventories are a means of discovering information such as the functionality and location of potentially reusable or releasable custom-developed code. Within 120 days of the publication date of this policy, each agency must update—and thereafter keep up to date—its inventory of agency information resources to include an enterprise code inventory that lists custom-developed code for or by the agency after the publication of this policy. Each agency's inventory will be reflected on Code.gov. 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 listed in this policy. Agencies shall fill out this information based on a metadata schema that OMB will provide on Code.gov.

7.3 Code.gov

Within 90 days of the publication date of this policy, the Administration will launch https://www.code.gov,[35] an online collection of tools, best practices, and schemas to help agencies implement this policy. The website will include additional materials such as definitions, evaluation metrics, checklists, case studies, and model contract language—with the goal of enabling collaboration across the Federal Government and advancing the Government's partnership with the public.

Additionally, Code.gov will serve as the primary discoverability portal for custom-developed code intended both for Government-wide reuse and for release as OSS. Note that Code.gov is not intended to house the custom-developed code itself; rather, it is intended to serve as a tool for discovering custom-developed code that may be available for Government-wide reuse or as OSS,

---

[33] *M-15-14: Management and Oversight of Federal Information Technology*, Office of Mgmt. & Budget, Exec. Office of the President, June 10, 2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf.

[34] Senior Agency Officials include positions that may include the Chief Acquisition Officer, Chief Operating Officer, Chief Financial Officer, Chief Technology Officer, Chief Data Officer, Senior Agency Official for Privacy, Chief Information Security Officer, and Program Manager.

[35] Code.gov will be modeled after Data.gov (https://www.data.gov) and Project Open Data (https://project-open-data.cio.gov/).

and to provide transparency into custom-developed code that is developed using Federal funds. This discoverability portal will be publically accessible and searchable via a variety of fields and constraints, such as the name of the project, its intended use, and the agency releasing the source code. Code.gov will evolve over time as a community resource to facilitate the adoption of good custom source code development, sharing, and reuse practices.

7.4 Code Repositories

Accessible, buildable, version-controlled repositories for the storage, discussion, and modification of custom-developed code are critical to both the Government-wide reuse and OSS pilot program sections of this policy. Agencies should utilize existing code repositories and common third-party repository platforms as necessary in order to satisfy the requirements of this policy.[36] Code.gov will contain additional information on this topic.

7.5 Licensing

Licensing is a critical component of OSS and can affect how the source code can be used and modified. Accordingly, when agencies release custom-developed code as OSS, they shall append appropriate OSS licenses to the source code. Additional information on licensing will be available on Code.gov.

7.6 Agency Policy

Within 90 days of the publication date of this policy, each agency's CIO—in consultation with the agency's CAO—shall develop an agency-wide policy that addresses the requirements of this document. For example, the policy should address how the agency will ensure that an appropriate alternatives analysis has been conducted before considering the acquisition of an existing commercial solution or a custom-developed solution. In accordance with OMB guidance,[37] these policies will be posted publicly. Moreover, within 90 days of the publication date of this policy, each agency's CIO office must correct or amend any policies that are inconsistent with the requirements of this document, including the correction of policies that automatically treat OSS as noncommercial software.

7.7 Accountability Mechanisms

Progress on agency implementation of this policy will be primarily assessed by OMB through an analysis of each agency's internal Government repositories, public OSS repositories, and code inventories on Code.gov, as well as data obtained through the quarterly Integrated Data

---

[36] Covered agencies should ensure access to these services. *See M-10-23: Guidance for Agency Use of Third-Party Websites and Applications,* Office of Mgmt. & Budget, Exec. Office of the President, June 25, 2010. https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

[37] *See M-15-14: Management and Oversight of Federal Information Technology*, Office of Mgmt. & Budget, Exec. Office of the President, June 10, 2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-14.pdf. This requires that IT policies be posted publicly at https://[agency].gov/digitalstrategy, and included as a downloadable dataset in the agency's Public Data Listing.

Collection (IDC), quarterly PortfolioStat sessions, the IT Dashboard, and additional mechanisms to be provided via Code.gov.[38]

[38] PortfolioStat is the core oversight tool used by OFCIO to improve both the efficiency and effectiveness of Federal IT. PortfolioStat's principle objectives are to serve as an overview of each agency's portfolio of IT investments and to oversee execution of OFCIO and OMB-wide policy. For information on the IT Dashboard, see https://itdashboard.gov/.

Appendix A: Definitions

Agency: For the purposes of this policy, an agency is one that meets the definition of executive agency under the Clinger Cohen Act of 1996. *See* 41 U.S.C. § 11101.

Code.gov: This platform is primarily intended to serve two distinct functions. First, it will act as an online collection of tools, guides, and best practices specifically designed to help agencies implement the framework presented in this policy. Second, it will serve as the primary discoverability portal for custom-developed code intended both for Government-wide reuse and for potential release as OSS. Code.gov is not intended to house the custom-developed code itself; rather, it is intended to serve as a tool for discovering custom-developed code that may be available for Government-wide reuse or as OSS, and to provide transparency into custom-developed code that is developed using Federal funds. This discoverability portal will be publically accessible and searchable via a variety of fields and constraints, such as the name of the project, its intended use, and the agency releasing the source code. Code.gov will be accessible at https://www.code.gov and will evolve over time as a community resource to facilitate the adoption of good custom source code development, sharing, and reuse practices.

Custom-Developed Code: For the purposes of this policy, custom-developed code is code that is first produced in the performance of a Federal contract or is otherwise fully funded by the Federal Government. It includes code, or segregable portions of code, for which the Government could obtain unlimited rights under Federal Acquisition Regulations (FAR) Pt. 27 and relevant agency FAR Supplements. Custom-developed code also includes code developed by agency employees as part of their official duties. For the purposes of this policy, custom-developed code may include, but is not limited to, code written for software projects, modules, plugins, scripts, middleware, and APIs; it does not, however, include code that is truly exploratory or disposable in nature, such as that written by a developer experimenting with a new language or library.

Mixed Source Software: A mixed source software solution incorporates both open source and proprietary code.

Open Source Software (OSS): Software that can be accessed, used, modified, and shared 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) and/or that meet the definition of "Free Software" provided by the Free Software Foundation (https://www.gnu.org/philosophy/free-sw.html).

Proprietary Software: Software with intellectual property rights that are retained exclusively by a rights holder (*e.g.*, an individual or a company).

Software: Refers to (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; and (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.[39]

Source Code: Computer commands written in a computer programming language that is meant to be read by people. Generally, source code is a higher level representation of computer commands as they are written by people and, therefore, must be assembled or compiled before a computer can execute the code as a program.

[39] As "computer software" is defined in 48 C.F.R. § 2.101. https://www.gpo.gov/fdsys/pkg/CFR-2002-title48-vol1/pdf/CFR-2002-title48-vol1-sec2-101.pdf.