OFFICE OF SYSTEMS/CHIEF INFORMATION OFFICER

OPEN SOURCE SOFTWARE ACQUISITION, MANAGEMENT AND USE POLICY

Version 2.0
Date: 4/19/2018

1. Purpose

Identify the policy for Open Source Software (OSS), Federal Reusable Software (FRS), Third Party Library usage, and related procurement considerations at the Social Security Administration (SSA).

The Office of Management and Budget (OMB) has directed agency Chief Information Officers (CIO) to develop a policy encouraging the use and sharing of Open Source code and reuse of Federal code. See M-16-21 Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software.

2. Background

The Second Open Government National Action Plan supports improved access to custom software code developed for the Federal Government, emphasizing that using and contributing to open source software stimulates innovation, lower costs, and benefits the public. In support of that commitment, OMB issued a policy (OMB M-16-21) to improve the way the Federal Government acquires and shares custom-developed Federal code.

The OMB policy states that: 1) agencies should make new custom code, that the Federal Government paid to develop, available for reuse across Federal agencies and, 2) the Federal Government must release a portion of new custom code to the public as OSS.

This policy will accomplish the following:

1. Provide guidance on software procurement considerations that you must make prior to acquiring custom-developed software.
2. Revise and replace the Office of System's Management Directive on Open Source dated October 3, 2011 policy on source code use in the agency.
3. Establish requirements for releasing code in the public domain as OSS and/or for Federal reuse.

3. Applicability

The policy applies to all software, source code, and systems developed, implemented, installed, procured, or managed by employees of the SSA, subject to certain exceptions noted below.

4. Exceptions

The policy does not require us to retroactively make existing custom-developed source code created by third party developers or vendors for the Federal Government available for Government-wide reuse or as OSS.

However, we strongly encourage making such code available for Government-wide reuse or as OSS, to the extent permissible under existing contracts or other agreements.

The policy also does not apply to proprietary software and code that the Federal Government did not pay to develop, even if later procured by the Federal Government (e.g., Microsoft Word).

5. Authority

We established this Policy under the authority of the Commissioner of Social Security Administration (COSS) as the agency head (see OMB M-16-21, Section 7.1). The COSS authorizes the CIO, in keeping with FITARA and OMB M-16-21, to establish our policy. The CIO, in consultation with the COSS, may alter, amend, or rescind this policy. The CIO may delegate the responsibility for this policy to an SES level executive.

As required by OMB M-16-21, the CIO will work with other Senior Agency Officials (SAO) and agency leadership to implement the requirements of this policy. Our SAOs include the Chief Financial Officer/Chief Acquisition Officer, SAO for Privacy, Component Security Officer, Chief Information Security Officer, etc. The CIO retains sole authority to alter, amend, or rescind this Policy. The CIO may delegate the responsibility of parts or all of this policy to a CIO designee.

The application of this policy is mandatory and applies to all components.

6. Requirements

6.1 OSS and FRS Software Procurement Consideration

When developing or acquiring custom code from a third party vendor, you must take into consideration contract language that will permit the Federal Government to reuse the code and release it to the public as Open Source. Additionally, we prohibit third party vendors from reselling code developed for us without consent.

Language must include, at a minimum, the following:

1. Require the third-party vendor to deliver the underlying custom source code, associated documentation, related files, build instructions, software user guides, automated test suites, and other associated documentation as applicable.
2. Secure unlimited rights to the custom source code, associated documentation, and related files – which include the rights to reproduction, reuse, and distribution of the custom source code, associated documentation, and related files across the Federal Government.

Information Technology Support Services contracts, mainly those that involve software development, should include contract language/clauses/terms and conditions that contain information regarding software/data rights restrictions whether that is with regular software programming languages or open source software.
Examples:

> 'Rights in Data - Special Works (DEC 2007)' - The Contractor **shall not** use, release, reproduce, distribute, or publish any data first produced in the performance of this contract, nor authorize others to do so, without written permission of the Contracting Officer.
>
> 'Rights in Data - General Works (DEC 2007)' - The Contractor **shall** have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—
>
> 1.
>   1. As prohibited by Federal law or regulation (e.g., export control or national security laws or regulations);
>   2. As expressly set forth in this contract; or
>   3. If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

If the contract will need to include language on OSS or data rights, it is important to determine which clause is applicable to that contract. The default should be 'Rights in Data – Special Works (DEC 2007).' You must obtain approval from the CIO to exclude this clause.

6.2 Leveraging OSS, FRS and Third Party Libraries

We advocate the use of OSS and FRS in systems or as tools in performing agency work. The decision to use software products of any origin (whether custom built, purchased, downloaded, or obtained by other means) is the assigned responsibility of the appropriate governance bodies and managerial/technical staff. You must make these decisions after consideration of all available options and after evaluation of alignment with architectural, budgetary, regulatory, and operational needs. The Open Source Staff will provide and maintain and guidance on agency best practices for leveraging open source and federally reusable software and code.

When introducing OSS or FRS into our environment or expanding the use in our products you must:

- Understand and follow the terms of the license.
- Ensure that the product fits into our technical architecture.
- Provide resources to manage the product as well as its version lifecycles.
- Provide needed maintenance resources.

6.2.1 Terms of OSS or FRS license must be understood and followed

Employees (otherwise known as "the responsible party") who use OSS or FRS are responsible for ensuring that everyone follows the terms of the license.

The terms of the license can restrict or otherwise control modifications of OSS or FRS (whether by SSA or by a vendor). The responsible party must ensure that changes to the code allow us to remain in compliance with the license agreement. You should consult the Office of General Council (OGC) before you make any OSS or FRS code modifications.

By using OSS or FRS, the responsible party binds us to the terms of those licenses and commits us to abide by those legal agreements. SSA is the licensee, not the responsible party, so the decision to enter into such agreements must consider issues and assign responsibilities to SSA as a whole.

Many licenses contain restrictions regarding how and when we can redistribute open software to an entity outside of SSA (Disability Determination Services' (DDS) are an example of such an entity). Some require that we maintain a clear trail of changes to copyrighted code in the program source documents. Nearly all licenses are based on the author's copyright, which prohibits un-attributed use of the author's work in other products. Failure to abide by these provisions can expose us and our business partners to a variety of legal claims.

Prior to entering into any OSS licensing agreement on behalf of SSA, the responsible party should submit the text of the license agreement, and an explanation of how they will use the product, to our OGC. If OGC finds the license terms to be acceptable, the responsible party can then proceed by following section 6.2.2. OGC can waive this requirement, but the responsible party cannot.

6.2.3 OSS Product and Version Lifecycles Must Be Managed

Software products (of any type) do not operate in isolation, but instead operate as parts of larger systems comprised of many other products and parts. Those interacting components are all subject to asynchronous change. Such changes (e.g., release of new versions or patches) are notorious for having unintended consequences and must therefore be thoroughly planned and tested before we implement them.

Whether building the solution, buying as a Commercial Off-The-Shelf (COTS) package, or leveraging open source software, responsible parties must ensure that adequate provisions have been or are going to be made for the ongoing lifecycle management of the software product.

6.2.4 Maintaining Open Source Software

There are two basic options available for providing the ability to maintain products:

1. When you are given the task of maintaining the product, you must manage the source code for that product in accord with our practices (i.e., source code supporting any and all used versions of the product must be managed through our standard source code tools used for the target execution environment, such as ENDEVOR, Integrity, etc.).
2. Arrange for separate, contracted maintenance support for the OSS. The support should be for the entire time you expect to use the product, should contain service level agreements to guarantee responsiveness, and should specify the mechanisms you will use to report and resolve issues.

6.2.5 Security Considerations for OSS

Implementing any software without appropriate maintenance and support can present a security risk. While OSS can be different from commercial software in various ways, the processes that determine intake and use must be the same for any software approved for use. When considering the use of OSS and FRS, you should follow our existing security processes documented in the Information Security Policy to ensure proper mitigation of risk.

6.2.6 Third Party Library Usage During Development

Agency code assets must use SSA's dependency management solution for third party libraries.

Developers are free to use any third party library versions except for:

1. Library versions with known Common Vulnerabilities and Exposures (CVEs) identified by a recognized standards body; or
2. Library versions that are end-of-life, retired, deprecated or no longer supported; or
3. Library versions that have been blacklisted by the agency

6.2.7 Third Party Library Usage Before Release and Deployment

Agency Code Assets must have their third party libraries scanned for CVEs prior to being deployed to any environment. Production deployment scan results must be saved by the deployment agent.

Agency Code Assets cannot be released to a production environment if they have a known critical CVE. If a Code Asset has a known critical CVE, but wishes to be deployed to a production environment, one of the following must occur:

1. The vulnerability is fixed; or
2. The reason why the vulnerability isn't being fixed is documented via a Plan of Action & Milestones (POA&M), tracked as a risk, and approved by the CISO, CIO, or designee

6.2.8 Third Party Library Usage Post Release and Deployment

Agency developed software must have its third party libraries scanned for CVEs on a monthly basis, at minimum.

When a CVE is identified in a production released/deployed version of agency developed software, the CVE must be remediated as soon as possible.

In order to keep the application running in production, one of the following must occur:

1. The vulnerability is fixed and deployed; or
2. The reason why the vulnerability isn't being fixed is documented via a Plan of Action & Milestones (POA&M), tracked as a risk, and approved by the CISO, CIO, or designee

6.3 Code Sharing

Sharing our custom-developed code outside the agency presents challenges and risks, however, participating in open source communities and leveraging the skills and knowledge of individuals across the Federal Government and beyond can result in enhancements to code quality and security, economic growth and innovation, and decrease duplicative acquisitions for the same code.

This policy lays out the guidelines to ensure we can make our custom-developed source code broadly available while protecting sensitive information and program policy.

To oversee and govern our open source and reuse policy and procedures, the CIO will assign responsibility to an OSS staff in the Office of Software Engineering (OSE). OSE may incorporate the staff within an existing division or established as a separate entity.

6.3.1 Exceptions to Federal Reuse or Open Source Publication

OMB has identified the exceptions that we may apply to exempt sharing custom code with other federal agencies or releasing as Open Source. See OMB M-16-21, section 6. Exceptions to Government Code Reuse.

The CIO has further clarified the OMB exceptions for our specific risks to agency mission, programs, or operations.

We are restricted from releasing code if the code would expose sensitive law, regulations, or policy or could potentially lead to fraud. Examples of software code that you should exclude from reuse include code that automates business policy or processes such as auditing, securing Personally Identifiable Information, or fraud detection. Additionally, you should exclude any

software code where the corresponding Program Operations Manual System instructions are deemed to be sensitive.

6.3.2 Sharing SSA code

OMB M-16-21 outlines best practices for participating in the Open Source Community. See OMB M16-21 section 5.

The OSS staff plays a key role in governance over sharing code.

As a rule, our developers will not engage in Open Development. If developing in the open will benefit the project, the developer should consult with the project manager and/or component manager. If management agrees, they will present the request to the OSS staff for consideration. The CIO or CIO designee will approve or deny requests.

6.3.2.1 Selection and Enterprise Code Inventory (ECI)

We will prioritize the custom-developed code that we release in the open based on its potential usefulness to the public.

OSS staff will identify potential candidate code from the pool of newly developed custom code and present options to the CIO or CIO designee, based on internal procedures.

The CIO or CIO designee will select the code that we will publish as Open Source. Agency code that disclose sensitive business, integrity, or security rules are prohibited from being released as open source.

OSS staff is responsible for creating and maintaining an Enterprise Code Inventory (ECI). The ECI is a list that contains a description of all custom code developed for or by the agency after the August 8, 2016 publication of OMB M-16-21.

The ECI will serve as a tool for discovering custom code that may be available for Federal reuse or as OSS. The inventory will not house the code. The inventory will indicate whether the code is available for Federal Reuse, OSS, or Restricted. See Code.gov for more information on the ECI.

6.3.2.2 Review, Publish, and Monitor

The OSS staff will conduct reviews of the code and documentation. Project developers, technical staff, technical experts, and OGC may have a role in reviewing the code before we publish it.

This CIO or designee will grant permission to OSS staff who will publish custom-developed code outside the agency firewall.

The OSS staff will monitor the repository for issues, questions, and suggestions for improvements.

7. Responsibilities

Responsibilities associated with the policy.

Roles	Responsibilities
Architecture Review Board (ARB)	• Ensure the compliance of the OSS and FRS to the our established architectural standards
Chief Information Officer (CIO)	• Establish and revise Open Source Code Policy as required by OMB. • Select code that we will release as OSS • Establish OSS staff • Designate OSS staff authority to publish code to an open source repository.
Open Source Software (OSS) Staff	• Create and maintain an ECI • Select potential candidate code for Open Source consideration • Present candidate code to CIO for decision. • Respond to questions, issues, and suggestion from the public or other Federal agencies
Office of Acquisitions and Grants (OAG)	• Ensure contracts include appropriate clauses
Office of Information Security (OIS)	• Ensure code coming into and out of the agency does not pose a security risk, or • Does not introduce addition/unacceptable security risk, or • Does not introduce additional unmitigated vulnerability
Office of the General Council (OGC)	• Advise personnel on issues related to OSS licensing

Change History

Version	Date	Reason for Change
1.0	11/6/2016	CIO-approved version

2.0	4/19/2018	Incorporated third party library usage. Miscellaneous corrections

Appendix A: Glossary

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.

Code.gov: An online repository of tools, guides, and best practices specifically designed to help covered agencies implement the framework presented in this policy. Code.gov will evolve over time as a community resource to facilitate the effective adoption of open source software.

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.

Development Division Tech: A Tech 14 or 15 from the division where the software was developed and maintained

Enterprise Code Inventory (ECI): A list that contains all custom code developed for or by us after the publication of the OMB policy on Source Code (date published 08/08/2016). It will serve as a tool for discovering custom code that may be available for Government-wide reuse or as open source software. The inventory will not house the code. The inventory will indicate whether the code is available for Federal Reuse, OSS, or Restricted.

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.

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).

Proprietary Software: Software with intellectual property rights that an individual or a company retains exclusively. Although an individual or a company (through the use of a proper open source license) can retain open source intellectual property rights, 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 "closed-source," in that its source code is not made broadly available to users or the general public without restrictions defined by the owner.

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.

Source Code: Information written in a computer programming language that is readable by people. A utility must interpret or compile source code 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.

Third Party Library: A reusable software component developed to be either freely distributed or sold by an entity other than the original vendor of the development platform.