Forest Service Manual
National Headquarters - Washington Office
Washington, DC

Forest Service Manual 6600 – Systems Management
Chapter 6630 - Software Source Code

Amendment: 6600-2019-1

Effective date: November 13, 2019

Duration: This amendment is effective until superseded or removed.

Approved by: Claudette Fernandez, Deputy Chief, OPS

Date approved: November 12, 2019

Responsible Staff:

Last Change: 6600-2018-3 to FSM 6685

Superseded Document(s):

Digest: Following is an explanation of the changes throughout the directive by section.

6630: This amendment establishes chapter, captions, codes, and sets forth direction for "Software Source Code."

Table of Contents

6630.1 - Authority

Clinger-Cohen Act of 1996, Title 40, United States Code, section 11101(6) (40 U.S.C. 11101(6). Formerly known as the Information Technology Management Reform Act, reforms acquisition laws and information technology management of the Federal Government.

The Federal Information Technology Acquisition Reform Act of 2014 (FITARA), Public Law 113-291 (Pub. L. 113-291). This act requires that the Office of Management and Budget (OMB) evaluate agencies' management and oversight of all federal information technology.

Privacy Act of 1974, Title 5, United States Code, section 552a (5 U.S.C. 552a). This act states in part, "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains...."

Freedom of Information Act (FOIA), Title 5 United States Code, section 552 (5 U.S.C 552). Enacted in 1966 and established for the first time an effective statutory right of access by any person or organization to federal government information.

OMB Memorandum M-13-13, Open Data Policy-Managing Information as an Asset, May 9, 2013. This memorandum requires agencies to collect or create information in a way that supports downstream information processing and dissemination activities.

OMB Memorandum M-15-14: Management and Oversight of Federal Information Technology, June 10, 2015. The purpose of this memorandum is to provide implementation guidance for the Federal Information Technology Acquisition Reform Act (FITARA) and related information technology (IT) management practices.

OMB Memorandum M-16-21: Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software, August 8, 2016. This memorandum improves the way Federal agencies buy, build, and deliver information technology (IT) and software solutions. When commissioning new custom software, this policy requires agencies to make custom code discoverable across all Government entities as Inner Source Software (ISS).

Departmental Regulation 3107-001, (DR 3107-001) Management of USDA IT Enterprise Initiatives. This Departmental Regulation (DR) establishes the U.S. Department of Agriculture (USDA) policy for identifying, evaluating, and designating information technology (IT) related enterprise initiatives in the form of a recommendation to the USDA Chief Information Officer (CIO). The intent of this DR is to promote the effective and efficient sharing of IT resources across the entire organization to drive down costs and improve customer service.

Departmental Regulation 3130-008 (DR 3130-008) Definition of Major Information Technology Investments. This DR provides policy guidance regarding major information technology (IT) investments for the U.S. Department of Agriculture (USDA) in accordance with the Office of

Management and Budget (OMB), Circular A-11 Preparation, Submission, and Execution of the Budget.

6630.2 - Objectives

Each year, the Federal Government spends more than $6 billion on software through more than 42,000 transactions. A significant proportion of software used by the Government is comprised of either pre-existing Federal solutions or commercial solutions. This directive aims to increase efficiency and decrease costs associated with these software purchases.

This policy abides direction set forth in the Federal Source Code Policy M-16-21 as well as U.S. Department of Agriculture directives that relate to Source Code. This document establishes the requirement to make computer code that was custom-developed for the Forest Service available for Government-wide reuse and to reuse other agencies' source code prior to commissioning new custom software development for the Forest Service. Further, it requires the release of at least 20 percent of new custom-developed code as Open Source Software (OSS).

6630.3 - Policy

This policy applies to all Forest Service employees, appointees, contractors and others who work for or on behalf of the Forest Service. This policy is effective upon issuance.

Contents stated within do not apply retroactively (for example, it is not required that existing custom-developed code be retroactively made available for Government-wide reuse or as Open Source Software (OSS)). However, such code available should be made available for Government-wide reuse or as OSS to the extent practicable.

It applies to all custom-developed codes that are first produced in the performance of a Federal contract or are otherwise fully funded by the Federal Government to address a business need. Custom-developed codes may include, but are not limited to, codes written for software projects, modules, plugins, scripts, middleware, and Application Programming Interfaces (APIs).

1. All software contracts for custom application development solutions in the Forest Service will include language that establishes Government data rights to custom-developed code, including, at a minimum, rights to Government-wide reusable software and rights to modify the code.

2. All custom-developed codes will be maintained in a Forest Service Associate Chief Information Officer (ACIO)-sanctioned Enterprise Source Code Management System. For more information about this tool, please visit CIO webpage.

3. All new custom-developed code must be made broadly available for Government-wide reuse across the Federal Government and will be discoverable through the Federal code portal (https://www.code.gov).

4. To support requirements set forth in the pilot program depicted in M-16-21, a minimum of 20 percent of all custom-developed code will be made publicly available as Open Source Software. When deciding which custom-developed code projects to release, the Forest Service should prioritize the release of custom-developed codes that it considers potentially useful to the broader community.

5. All custom-developed codes for the Forest Service will include documentation that describes the function, input, and output of the module, security, and any other information relevant to its reuse.

6. All authorized versions of compiled software and deployment packages for the Forest Service will be placed in an ACIO-sanctioned Enterprise Definitive Media Library (DML) as part of release process.

6630.31 - Policy Exceptions

Exceptions to this policy used must be approved and documented by the ACIO for the purposes of ensuring effective oversight and management of information technology resources.

For excepted software, Forest Service must provide to the Office of Management and Budget (OMB) a brief narrative justification for each exception, with redactions as appropriate. To examine exceptions furthers, refer to M-16-21 section 6.

Applicable exceptions are as follows:

1. The sharing of the custom-developed 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 custom-developed code would create an identifiable risk to the detriment of national security, confidentiality of Government information, or individual privacy,

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

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

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

6630.4 - Responsibility

6630.41 - U.S. Department of Agriculture Associate Chief Information Officer (ACIO) for Natural Resources and Environment

The Associate Chief Information Officer (ACIO) as the senior information resource management official for the Forest Service, has the responsibility to:

1. Issue Government-wide reusable software procedures and practices, establish procedures and approvals for the three-step strategic solutions analysis process, and establish, and enforce security standards for releasing Government-wide reusable software.

2. Ensure users have assistance when determining what code is reusable.

3. 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.

4. Establish accurate Government-wide reusable software inventories and maintain them.

5. Establish a data collection site that provides metrics to gauge the performance and reporting on Government-wide reusable software programs.

6. Maintain an inventory of all custom-developed code with Development, Modernization, and Enhancement (DME) activity.

7. Prioritize the release of custom-developed code that it considers potentially useful to the broader community.

8. Collect statistics on source code policy compliance annually.

9. Propose candidate custom-developed code projects for exemptions to this policy.

10. Review and renew any previously-approved policy exceptions annually.

11. Prepare language for Government-wide reusable software and custom-developed code requirements in software acquisition contracts or agreements whenever possible.

12. Ensure Program Managers work with Contracting Officers to incorporate sufficient language in solicitations and contract documents in order to obtain Government data rights to custom-developed code.

13. Train program personnel to appropriately administer contracts and employ practices that secure the full scope of the Government’s rights, including, but not limited to, sharing and using the code with other Federal agencies.

6630.5 - Definitions

Custom-Developed Code. Custom-developed code is first produced in the performance of a Federal contract or is otherwise fully funded by the Federal Government. This includes code, or 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.

Definitive Media Library (DML). The DML is the master repository for all definitive, authorized versions of compiled software and deployment packages. The DML provides the protected storage area for packages ready for deployment which will provide a single and comprehensive source for deployment and recovery.

Developer. A person or organization that designs and writes software and/or software applications. The term generally refers to the commercial software field, but it may also refer to employees creating internal applications within an enterprise. A developer implies more than just coding. Developers are typically involved with the user interface as well as the programming, although one person may not be responsible for both.

Enterprise Source Code Management System. A version control system designed to track changes in source code and other text files during the development of a piece of software. This allows the user to retrieve any of the previous versions of the original source code and the changes which are stored.

Information Technology (IT). Includes computers, ancillary equipment, software, firmware and similar procedure services (including support services), and related resources. However, it does not include any equipment that: (1) is acquired by a contractor incidental to a contract or (2) contains imbedded information technology (IT) that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, heating, ventilation, and air conditioning (HVAC) equipment, such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, are not IT as defined by Title 48, Code of Federal Regulations, Part 2, subpart 2.101

Inner Source Software or Government-wide reusable software. Non-sensitive software developed internal to the Forest Service which can be utilized across multiple teams across Federal agencies and accessed only by Federal agencies. Government-wide reusable software will aid in reducing redundant development, and can improve quality and performance of code. Government-wide reusable software remains under the protection and control of the Forest Service or appropriate Government agency and is not available as open source.

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 which meets the definition of "Free Software" provided by the Free Software Foundation.

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

Redact. Removal of information that is often personal (or possibly actionable) from a document.
Redacted document. A document that has had sensitive information removed or expunged.
Software. Refers to:

1. Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which they are recorded, that allow or cause a computer to perform a specific operation or series of operations and

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

System Owner. Officials having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

Version control. A category of processes and tools designed to keep track of multiple different versions of software, content, documents, websites and other information in development.

6630.6 - Abbreviations and Acronyms

The abbreviations and acronyms for the terms used in this chapter are:

ACIO - Associate Chief Information Officer

API - Application Programming Interfaces

DML- Definitive Media Library

OSS - Open Source Software

ISSO - Information System Security Officer

OMB - Office of Management & Budget

6631 - Custom Developed Code

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 Application Programming Interfaces. However, it does not include code that is truly exploratory or disposable in nature, such as code that is written by a developer experimenting with a new language or library.

Examples of custom-developed code include:

1. All application code and dependencies (libraries, static content, and so forth).

2. Any script used to create database schemas, application reference data, and so forth.

3. Environment creation tools and artifacts.

4. Any file used to create containers (Docker).

5. All supporting automated tests and any manual test scripts.

6. Any script that supports code packaging, deployment, database migration, and environment provisioning.

7. Configuration files.

8. No Secrets, User names, passwords, servers names should be in the source code.

9. Any other script or configuration information required to create infrastructure that supports multiple services (for example, enterprise service buses, database management systems, Domain Name System zone files, configuration rules for firewalls, and so forth).

6632 - Three-Step Software Solution Analysis

As defined in section 3 of M-16-21, the three-step software solutions analysis includes:

- ***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.

- ***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.

- ***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.

6633 - Sharing America's Code (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 Open Source Software (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 is publicly 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.

6634 - Information Resource Employees

6634.41 - Information Systems Security Officer (ISSO)

Forest Service Information Systems Security Officers (ISSO) who are assigned to the system are responsible for reviewing exemptions to the sharing of custom-developed code based on security restrictions and include supporting documentation prior to submission to the Associate Chief Information Officer for technical review. For a list of appropriate exceptions, refer to M-16-21 section 6.

6634.42 - System Owners

System owners shall ensure that:

1. Development teams identify, document, and review all custom-developed code prior to its release.

2. Custom-developed code is reviewed for security vulnerabilities, sensitive information, Personally Identifiable Information (PII) and other cyber mandates prior to its release as Open Source Software or Government-wide reuse and recommend exemptions when warranted.

3. Custom developed code is maintained and is functional throughout its lifecycle and make updates to the code as needed.

6634.43 - Development Teams

Development teams shall:

1. Identify custom-developed code that will be used for Government-wide reuse and Open Source Software programs.

2. Document all custom-developed code and software packages so that they include the code itself, at a minimum, as well as the following information:

   a. Status of software (prototype, alpha, beta, release);

   b. Intended purpose of software;

   c. Expected engagement level (how frequently the community can expect Agency activity);

   d. License details if applicable; and

   e. Any other relevant technical details on how to build, make, install, or use the software, including dependencies (if applicable).

3. Review custom-developed code for security vulnerabilities, sensitive information, and Personally Identifiable Information (PII) prior to its release as Open Source Software or Government-wide reuse and recommend exemptions when warranted.

4. Ensure that released custom-developed code is placed in the appropriate Associate Chief Information Officer-sanctioned media library and/or repository.