wiley

ALERT

OMB Releases Final Memorandum Emphasizing Open Source Software Requirements

August 9, 2016

WHAT: The Office of Management and Budget (OMB) released a Final Memorandum for the Heads of Departments and Agencies requiring that new custom-developed Federal source code be made broadly available for reuse across the Federal Government. The 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 over the next three years as Open Source Software (OSS).

WHEN: Effective August 8, 2016; each agency is required to develop agency-wide policies within 90 days that address these requirements.

WHAT DOES IT MEAN FOR INDUSTRY: With certain exceptions mostly related to national security, this Policy has the potential to re-shape how the Federal Government procures software solutions. The Policy contains a stated preference for existing Federal software solutions or existing commercial solutions, before considering custom software solutions. Additionally, the policy requires that agencies that enter into contracts for development of custom software must, *at a minimum*, "acquire and enforce rights sufficient to enable Government-wide reuse of custom developed code." Additionally, for the next three years, each agency is required, pursuant to a pilot program, to release at least 20 percent of its custom-developed code as OSS, prioritizing the code it considers to be potentially useful to the broader community.

Authors

Scott A. Felder
Partner
202.719.7029
sfelder@wiley.law

Practice Areas

Government Contracts

Intellectual Property

Patent and Data Rights Counseling and Disputes

OUR ANALYSIS:

On August 8, 2016, OMB released a Memorandum titled "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software." The purpose of the Memorandum is to improve procurement and delivery of Federal Information Technology (IT) and software solutions to "better support cost efficiency, mission effectiveness, and the consumer experience with Government programs." To that end, the Memorandum highlights that custom-developed source code often is not made broadly available for Federal Government-wide reuse, especially where agencies have difficulty establishing that the software code was produced in the performance of a government contract. As a result, the Memorandum asserts that the Federal Government duplicates acquisitions of substantially similar code in a manner that is inefficient for taxpayer dollars. The Memorandum highlights that there is precedent for this course of action; several departments and agencies have already made certain portions of source code publically available.

The Memorandum contains several key components. First, the Memorandum articulates a clear preference for meeting agency software needs by leveraging existing solutions, such as pre-existing Federal software solutions or commercial software solutions. After the Agency has concluded that an existing solution cannot adequately satisfy its needs, it may consider procuring custom-developed code in whole or in conjunction with pre-existing software code. Throughout these considerations, agencies are tasked with considering a range of identified concerns, including modular architecture, cloud computing, and open standards.

Second, the Memorandum requires the agencies acquire and enforce rights sufficient to enable Government-wide reuse of custom-developed code. "Custom-developed code" is broadly defined for purposes of the Memorandum as code "***first produced*** in the performance of a Federal contract or is otherwise fully funded by the Federal Government," and code, or segregable portions of code, for which the Government is entitled to unlimited rights under applicable regulations. Agencies must also maintain an inventory of all new code that is custom-developed for the Federal Government, and make that inventory discoverable in a new repository at www.code.gov.

Third, the Memorandum directs the establishment of a three-year pilot program, pursuant to which each agency is required to release no less than 20 percent of its new custom-developed code as Open Source Software (OSS). In fact, agencies are strongly encouraged to release as much custom-developed code as possible into open source communities "to further the Federal Government's commitment to transparency, participation, and collaboration." This code will be made available to the public with the stated goal of improving and contributing to existing OSS projects.

There are several exemptions and exceptions to the application of this Memorandum's requirements. Critically, source code developed for National Security Systems (NSS), as defined in 40 U.S.C. § 11103, is entirely exempt from the requirements set forth in the Memorandum. The term "National Security System means a telecommunications or information system operated by the Federal Government, the function, operation, or use of which

(A) involves intelligence activities;

(B) involves cryptologic activities related to national security;

(C) involves command and control of military forces;

(D) involves equipment that is an integral part of a weapon or weapons system; or

(E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.

(2) Limitation.–Paragraph (1)(E) does not include a system to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

40 U.S.C. § 11103(a).

Additionally, these policies do not apply retroactively to require that existing source code be made available for Government-wide reuse, although such availability is "strongly encouraged." Finally, the Memorandum lists several categories of exceptions that exempt an agency from sharing custom-developed code with other government agencies—***although these exceptions do not apply to the three-year pilot program***. These exceptions include:

- source code protected by patent or intellectual property law, the Export Administration Regulations, the International Traffic in Arms Regulations, and laws governing classified information;
- source code whose sharing would create an identifiable risk to detriment of national security, confidentiality of Government information, or individual privacy;
- source code whose sharing would create an identifiable risk to stability, security, or integrity of an agency's systems or personnel
- source code whose sharing would create an identifiable risk to agency mission, programs, or operations; or
- source code that the CIO believes is in the "national interest" to exempt sharing.

Wiley Rein will continue to monitor developments in this area and is available to assist clients regarding these issues.