U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Issue Date: 10/19/2017

Policy Directive 142-04

MEMORANDUM FOR: Component Heads

FROM: Chip Fulghum
Deputy Under Secretary for Management

SUBJECT: DHS Reusable and Open Source Software (OSS) Framework

This Policy Directive defines the Department of Homeland Security (DHS), Office of the Chief Information Officer (OCIO) activities and provides roles and responsibilities to ensure compliance with the Office of Management and Budget (OMB) Memorandum M-16-21, "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software."

In August 2016, OMB released M-16-21, which seeks to ensure that new custom-developed federal source code be made broadly available for reuse across the government. The memorandum also requires agencies, when commissioning new custom-developed code, to release at least 20 percent of new custom-developed code as Open Source Software for three years, and to collect data concerning new custom software to measure performance. This approach is consistent with the DHS Directive 262-06[1], "Digital Government Strategy" approach, which enables federal employees to work together within DHS and across other agencies to reduce costs, streamline development, apply uniform standards, and ensure consistency in creating and delivering information.

The DHS Chief Information Officer (CIO) is responsible for the developing, maintaining, disseminating, and implementing new policy and instructional requirements of M-16-21. The following actions are assigned to the DHS CIO:

- Inventory, on a continuing basis, all DHS custom-developed code and related information and publish a machine-readable source code project inventory that conforms to the code JavaScript Object Notation (json) schema for cataloging metadata on https://www.code.gov.
- Publish this policy on www.dhs.gov/digitalstrategy.
- Ensure that all new information technology (IT) with noncompliant software requires justification, and that the resulting contracts include provisions to ensure delivery of custom-developed code, documentation, and other associated materials from the developer throughout the development process.

[1] DHS Directive 262-06 implements OMB's Digital Government: Building a 21st Century Platform to Better Serve the American People, dated May 23, 2012

- Provide guidance around standard version control systems and a centralized software repository as identified by the Office of the Chief Information Officer's Office of the Chief Technology Officer, allowing for future compliance via automation.
- Annually, beginning Fiscal Year (FY) 2018, DHS will commence planning and coordination to implement the following activities as soon as practicable:
    - Release a minimum of 20 percent of custom-developed code as Open Source Software each year. The percentage is based on the total number of code projects in the inventory.
    - In coordination with the Office of the Chief Procurement Officer (OCPO) and Office of the General Counsel (OGC), develop and implement a policy or process that requires DHS to apply the three-step Software Solutions Analysis during the procurement phase for new IT systems. When contracting for developer services, DHS encourages vendors to use OSS, open standards, and modular architecture that meets DHS standards for security, federal interoperability, and data integrity wherever possible.
    - In coordination with the Science and Technology Directorate (S&T), OCPO, OGC, and other stakeholders, develop and implement a process that ensures appropriate rights to custom-developed code, recognizing that a vast majority of code produced for DHS is written by contractors. In order to increase the percentage of delivery of source code using free and open licensing, the CIO works with the OMB code.gov and OGC Intellectual Property (IP) to develop core contract language to disseminate within the Department. DHS CIO, in coordination with OCPO, OGC, and other stakeholders, ensures appropriate contract language, and a mechanism to ensure that delivered software meets contractual requirements, is in place.

This policy requires DHS Components to account for their custom-developed code, facilitate government-wide code reuse, and publish a portion of their custom-developed code as open source in accordance with OMB M-16-21 including:

- A new baseline of software development and acquisition that supports a “default to open” approach as it promotes the Department's vision of appropriate transparency;
- A posture of “default to open” requiring justification for noncompliant software, and ensuing delivery of custom-developed code, documentation, and other associated materials from the developer throughout the development process;
- A dissemination process for custom-developed code and related information that maximizes its availability to all other federal agencies, subject to limited exceptions, and that is the responsibility of the organization releasing code;
- An adherence to releasing a portion of custom-developed code as OSS through a public-facing software version controlled platform in a manner whereby any party can contribute new code, modify existing code, or make other suggestions to improve the software through the software development lifecycle;
- Contracts that must follow OMB's three-step software analysis outlined in M-16-21 and include contract requirements for OSS, open standards, and modular architecture requirements when applicable. Contracts for custom-developed code must also acquire and enforce rights sufficient to enable government-wide (or perhaps public) reuse of custom-developed code; and

- The inclusion of a metadata file in each project's source code repository. The metadata file will contain information about the project that can be included in the Department's code inventory.

The exceptions provided below may be applied, in specific instances, to exempt the Department from sharing custom-developed code with other government agencies. Any exceptions used are approved, in consultation with OGC, and documented by the DHS CIO (and provided to OMB) 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;
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 Department's systems or personnel;
4. The sharing of the source code would create an identifiable risk to the DHS mission, programs, or operations; or
5. The DHS CIO believes it is in the national interest to exempt sharing the source code.

More information about the implementation of these requirements will follow. Any questions regarding this Policy Directive Memorandum, please contact Michael Hermus, Executive Director of the Office of the Chief Technology Office at (202) 343-4421 or Michael.Hermus@hq.dhs.gov.