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

Homeland
Security

Revision 02
Issue Date: 9/12/2023
Expiration Date: 9/12/2025

Policy Directive 142-04

MEMORANDUM FOR: Distribution

FROM: R.D. Alles
Deputy Under Secretary for Management

RANDOLPH D ALLES
Digitally signed by RANDOLPH D ALLES
Date: 2023.09.12 10:56:10 -04'00'

SUBJECT: DHS Reusable and Open Source Software

This Policy Directive defines the responsibilities and authorities of the Department of Homeland Security (DHS), Office of the Chief Information Officer (OCIO), to ensure compliance with the 2016 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" and to promote a modern software environment across the Department. This memorandum asserts that new custom-developed, federal source code[1] be made broadly available for reuse across the Federal government. Policy Directive 142-04 is consistent with DHS Directive 262-06 "Digital Government Strategy" and the White House "Digital Government Strategy."

In support of M-16-21, I am directing the DHS Chief Information Officer (CIO) to implement the following:

1. Publish this policy on www.dhs.gov/open-source along with related guidance and reference materials related to the proper management and use of Open Source Software (OSS)[2].

2. Inventory, on a continuing basis, all DHS custom-developed source code and related information using the OMB code.gov Metadata Schema specification and publish it under a top-level DHS gov domain. This Source Code Inventory Process (SCIP),

[1] Source code is the human-readable, uncompiled version of software written in a programming language as plain text. The term "custom-developed" in this context refers to source code written specifically for a Department of Homeland Security software system versus for commercial purposes. This applies to entire IT systems, plug-ins or modules for existing commercial software, or low-code workflows and integrations.

[2] Open Source Software (OSS) is any code that is published publicly, accessible to anyone, and has a license attached allowing unlimited reuse of the software. Not all "source code" is OSS (for example, most commercial software products are not), and although there are some contrary examples, most OSS includes the products "source code" as a component (along with documentation, binary executables, build scripts, configuration, etc.).

available at: www.dhs.gov/scip, must set forth the tools, processes, policies, and mechanisms for the inventory of existing and new DHS custom-developed source code, including the:

a. DHS custom source code inventory metadata requirements for classified and unclassified systems including DHS-specific metadata that must be included with required code.gov metadata;

b. process for submitting DHS custom source code metadata for inventory in the Department code inventory file; and

c. requirements and processes for re-evaluation of the inventory on a periodic basis no longer than 12 months.

3. Develop and implement a default-to-open-source policy that requires new DHS custom-developed source code to be released as OSS, unless justified through an exception process. Support this policy directive (142-04) – and the use of open source projects within DHS custom-developed source code – by creating, publishing, and promoting, guidance on:

a. a process for releasing DHS custom-developed source code as OSS;

b. the exception process for not releasing DHS custom-developed source code as OSS;

c. determining the cybersecurity, supply chain, and privacy risks of DHS custom-developed source code intended for OSS release per DHS Office of the Chief Information Security Officer (OCISO) and DHS Chief Privacy Officer recommendations, including code attestation, provenance determinations, and foreign oversight, control, and influence (FOCI) concerns;

d. security best practices for use of external source code, whether open source or from other Federal agencies, within DHS custom-developed source code in coordination with DHS OCISO;

e. identifying and addressing legal issues associated with DHS custom-developed source code intended for OSS release including licensing, intellectual property, export controls, and technical transfer in consultation with the DHS Office of General Counsel (OGC), the DHS Export Controls Group, and the DHS Office of the Chief Procurement Officer (OCPO);

f. mechanisms related to the public-facing DHS open source repository including account creation and usage;

g. best practices and processes for maintaining open source repositories, including feature updates, bug fixes, patching of dependencies, and handling contributions; and

h. best practices for archiving open source repositories where DHS has identified it will no longer maintain them, including considerations for external entities that may be affected.

4. Release DHS OSS through the DHS OCIO public-facing software version control platform at www.github.com/dhs-gov, or a suitable component-specific platform, in a manner that permits the public sharing of the source code and, at the discretion of the developer, optionally permits contributions by non-DHS developers.

5. Collaborate with OGC, OCPO, and the DHS Chief Privacy Officer to develop guidance for contracts that involve new custom-developed source code to ensure that the government gains all rights necessary to publish such code as open source, unless justified through an exemption process, and includes relevant Open Source and other distribution clauses.

6. Require programs to follow the OMB Three-Step Software Solutions Analysis, set forth in M-16-21, for new information technology systems. This analysis is intended to leverage existing solutions, while mitigating duplicative spending. This process can be summarized as:

a. Step 1: requiring programs to conduct strategic analysis and analyze alternatives to any custom-code development, giving preference to use of existing federal software solutions;

b. Step 2: requiring programs to consider the use of Commercial Off The Shelf (COTS) software before considering developing custom source code if existing federal software solutions do not efficiently and effectively meet program needs;

c. Step 3: requiring programs to consider publishing custom code as OSS; and

d. throughout the process, programs should consider open standards and modular architectures that meets standards for security, federal interoperability, and data integrity wherever possible.

7. Make DHS custom-developed source code available to other Government agencies (if not open sourced) unless a specific exception applies. Any exceptions to government reuse used must be approved and documented by the DHS CIO, in consultation with the Chief Privacy Officer, for the purposes of ensuring effective oversight and management of information technology resources. For excepted software, agencies must provide OMB a brief narrative justification for each exception, with redactions as appropriate. Applicable exceptions must follow the exceptions listed in

section 6 of M-16-21.

8. Support open source supply chain security by encouraging DHS programs and personnel to contribute directly to OSS projects that DHS relies upon, by developing and publishing guidance on:

a. how programs should select appropriate projects to contribute to in support of the DHS mission;

b. reasonable legal and privacy checks for open source contributions, in coordination with OGC and DHS Chief Privacy Officer;

c. reasonable security precautions, in coordination with OCISO;

d. how DHS programs may incentivize contributions to OSS projects; and

e. other steps that programs and personnel should take when making open source contributions, in coordination with OGC.

Additional information and guidance related to the implementation of these requirements will be published on www.dhs.gov/open-source. For any questions regarding this Policy Directive, please contact the Offfice of the Chief Technology Officer (opensource@hq.dhs.gov) within the Office of the Chief Information Officer.