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

Homeland Security

Revision 01
Issue Date: 08/17/2021
Expiration Date: 08/17/2023

Policy Directive 142-04

MEMORANDUM FOR: Component Heads

FROM: R.D. Alles
RANDOLPH D ALLES
Digitally signed by RANDOLPH D ALLES
Date: 2021.08.17 09:57:08 -04'00'
Deputy Under Secretary for Management

SUBJECT: DHS Reusable and Open Source Software

This Policy Directive defines the Department of Homeland Security (DHS), Office of the Chief Information Officer (OCIO) activities 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." This memorandum establishes that new custom-developed, federal source code 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 OCIO Memorandum "Open Source Software Compliance."

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

1. Inventory, on a continuing basis, all DHS custom-developed source code and related information using OMB's code.gov Metadata Schema specification and publish this inventory to OMB's code.gov repository;

2. Publish this policy on www.dhs.gov/digitalstrategy;

3. Support a default-to-open-source approach that requires new DHS custom-developed source code to be released as Open Source Software (OSS) unless justified through an exception process;

4. Collaborate with the DHS Office of the General Counsel (OGC), the DHS Office of the Chief Procurement Officer (OCPO), and DHS Chief Privacy Officer to develop guidance, for use in preparing contracts that involve new custom-developed source code such that the government gains distribution rights unless justified through an exemption process, and includes relevant Open Source and other distribution clauses;

5. Release DHS OSS through the DHS OCIO's public-facing software version control platform in a manner that permits the public sharing of the source code and, at the discretion of the developer, optionally permits the modification of source code by non-DHS developers;

6. Require contracts to follow the OMB three-step Software Solutions Analysis, set forth in M-16-21, during the procurement phase for new information technology systems. This analysis:

    a. requires contracts to consider existing OSS prior to any custom-code development;

b. requires contracts to consider the use of Commerical Off The Shelf (COTS) before considering developing custom source code if existing OSS code is not available; and

c. encourages contracts to use OSS, open standards, and modular architectures that meets DHS standards for security, federal interoperability, and data integrity wherever possible.

7. Plan, coordinate, and develop a DHS Source Code Inventory Process (SCIP) that sets forth the:

   a. process of inventory related to DHS custom-developed source code;

   b. guidance on tools, processes, policies, and mechanisms for the inventory of existing and new DHS custom-developed source code;

   c. exemptions for releasing DHS custom-developed source code as OSS;

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

   e. process for submitting DHS custom-code metadata for inventory;

   f. process surrounding the release of DHS custom-developed source code as OSS;

   g. governance identifying and addressing legal issues surrounding DHS custom-developed source code intended for OSS release including licensing, intellectual property, export controls, and technical transfer per OGC and OCPO recommendations;

   h. policy for determining the security and privacy risk 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; and

   i. mechanisms surrounding the public-facing DHS open source repository including account creation and usage.

8. Make new custom-developed source code available to other Government agencies unless a specific exemption applies. Any exceptions used must be approved and documented by the DHS CIO, in consultation with OGC and the DHS Chief Privacy Officer, and documented by the DHS CIO (and provided to OMB with redactions, as appropriate) for the purposes of ensuring effective oversight and management of information technology resources. Applicable exceptions are as follows:

   a. The sharing of the source code is restricted by law or regulation;

   b. The sharing of the source code would create an identifiable risk to the detriment of national security, confidentiality of government information, or individual privacy;

   c. The sharing of the source code would create an identifiable risk to the stability, security, or integrity of the Department's systems or personnel;

d. The sharing of the source code would create an identifiable risk to the DHS mission, programs, or operations; and/or

e. 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. For any questions regarding this Policy Directive Memorandum, please contact the DHS Chief Technology Officer, Office of the Chief Information Officer.