INFORMATION TECHNOLOGY

DOD Needs to Fully Implement Program for Piloting Open Source Software

GAO Highlights

Why GAO Did This Study

Open source software is code that is released under a license which grants users the right to modify, share, and reuse the software. Making code available for reuse as open source can have major benefits such as decreasing costs and improving efficiencies. The National Defense Authorization Act for Fiscal Year 2018 required DOD to submit a plan to Congress for initiating the open source software pilot program established by OMB memorandum M-16-21. DOD submitted its plan to Congress in June 2018.

The act includes a provision for GAO to report on DOD's implementation of the open source software pilot program. GAO's objectives were to (1) assess the extent to which DOD has implemented the open source software pilot program and other related requirements established by OMB; and (2) describe the views of responsible DOD officials on the use of open source software to achieve efficiency, transparency, and innovation at the department. To address these objectives, GAO compared DOD's plan for implementing the program to OMB's memo. GAO also interviewed defense officials at 11 DOD components including military departments, and defense agencies on their views about the benefits and risks of making code available as open source software.

What GAO Recommends

GAO is making four recommendations to ensure DOD implements the program and develops milestones for completing requirements in the OMB memo. DOD agreed with two but did not agree with one and partially agreed with another. As discussed in this report, GAO maintains that all recommendations are needed to satisfy the act.

What GAO Found

The Department of Defense (DOD) has not fully implemented an open source software pilot program and related Office of Management and Budget (OMB) requirements as mandated by the National Defense Authorization Act for Fiscal Year 2018. OMB memorandum M-16-21 calls for agencies to implement a pilot program, which it defines as (1) releasing at least 20 percent of new custom developed code as open source, and (2) establishing a metric for calculating program performance. However, DOD has not fully implemented the program and has not established the metric. The OMB memorandum also requires agencies to implement other supporting activities. These include issuing policy on government-wide use of code, conducting analyses of software solutions, securing data rights and inventory code, and facilitating the open source community. DOD has not implemented the policy requirement and has partially implemented the remaining three requirements.

- Regarding the policy and analysis requirements, DOD plans to issue a policy and conduct analyses by the end of the 2019 calendar year. If the department effectively implements these intended steps consistent with OMB direction, DOD should be able to fully address these requirements.
- For the requirement of securing data rights and inventorying code, DOD issued a memorandum that directs contracting officers to secure data rights and to identify all source code created after August 2016. However, DOD's components have not executed these activities nor has DOD identified a milestone for when they will be completed.
- For the facilitating community requirement, DOD issued a memorandum that encourages conversations to foster communities and allow others to contribute knowledge, among other initiatives. However, DOD has not fully engaged in open development, established a release schedule, or fully documented its source code to facilitate use and adoption. To address these areas, DOD's Chief Information Officer plans to issue guidance but has not established a milestone for doing so.

Until DOD fully implements the pilot program and develops milestones for two of the four OMB requirements (secure data rights and inventory code, and facilitate community), it will not be positioned to satisfy the mandate established in the law.

DOD officials from 11 components expressed their opinions that an open source pilot program would potentially result in financial benefits and increased efficiency. However, there were disparate views on how to manage the cybersecurity risk of using open source software. Specifically, officials from three components noted that security concerns could result in the sporadic use of OSS, whereas eight officials stated that the potential cybersecurity risks were managable.

_____ **United States Government Accountability Office**