United States Government Accountability Office

Report to Congressional Committees

September 2019

INFORMATION TECHNOLOGY

DOD Needs to Fully Implement Program for Piloting Open Source Software

Accessible Version

GAO-19-457

September 2019

INFORMATION TECHNOLOGY

DOD Needs to Fully Implement Program for Piloting Open Source Software

GAO Highlights

Highlights of GAO-19-457, a report to congressional committees

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.

View GAO-19-457. For more information, contact Carol Harris at (202) 512-4456 or HarrisCC@gao.gov.

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.

Contents

Table

Abbreviations

CIO	Chief Information Officer
COTS	commercial off-the-shelf
DOD	Department of Defense
OMB	Office of Management and Budget
OSS	open source software

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 10, 2019

Congressional Committees

The federal government spends billions of dollars on software each year. A significant proportion of software used by the Government is comprised of either preexisting Federal solutions or commercial solutions. These solutions include, among others, open source software (OSS). OSS is software developed from source code that is obtained under a license that allows it to be modified, shared, and reused.[1] When Federal agencies are unable to identify an existing Federal or commercial software solution that satisfies their specific needs, they may choose to develop a custom software solution on their own or pay for its development. However, when agencies procure custom-developed source code they do not necessarily make their new code broadly available as OSS for government-wide reuse. According to the Office of Management and Budget (OMB), even when agencies are in a position to make their source code available on a government-wide basis, they do not make such code available to other agencies in a consistent manner. These challenges may result in duplicative acquisitions for substantially similar code and an inefficient use of taxpayer dollars.

On August 8, 2016, OMB issued memorandum M-16-21[2] that established requirements for federal agencies to improve the way they buy, build, and deliver software solutions through the use of OSS code. The memorandum called for the agencies to implement an OSS pilot program and establish other associated requirements to implement the pilot program.

Enacted on December 12, 2017, the National Defense Authorization Act for Fiscal Year 2018 mandated that the Secretary of Defense initiate the

[1]Agreeing to an OSS license allows an individual, company, or government entity to replicate, distribute, and run the OSS application as often and as broadly as desired, to obtain its human-readable source code, and, subject to release requirements that vary from license to license, to expand or extend the OSS application. Payment for OSS is indirect, consisting in most cases of agreeing to share value in the form of application fixes and extensions with the community that maintains the application.

[2]OMB, *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software (M-16-21),* Aug. 8, 2016.

OSS pilot program established by the OMB memorandum within 180 days (by June 10, 2018).[3] Further, the act required the department to report to Congress within 60 days (by February 10, 2018) with details of its plan. The plan was to identify candidate software programs, selection criteria, intellectual property and licensing issues, and any other matters determined by the Secretary.

The act also included a provision that we report to Congress no later than June 1, 2019, on DOD's implementation of the OSS pilot program. Our objectives were to: (1) assess the extent to which DOD has implemented the OSS pilot program and other related requirements established by the OMB memorandum; and (2) describe the views of responsible DOD officials on the use of OSS.

To address the first objective, we selected six requirements from the OMB memorandum titled the *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source software (M-16-21, Aug.8, 2019)* that we determined were needed to establish an OSS pilot program. Two requirements establish the pilot program: (1) releasing at least 20 percent of newly custom-developed code each year as OSS for the term of the pilot program, and (2) developing a metric to gauge the performance of the pilot program. The other four requirements support the implementation of the pilot program: (1) issuing an OSS policy, (2) conducting an OSS analysis, (3) securing data rights and inventorying custom code, and (4) facilitating the OSS community. We met with officials from the Office of the DOD Chief Information Officer (CIO) and the Defense Digital Service to discuss the status of the department's implementation of the OSS pilot program. To determine the extent to which the pilot program had been implemented, we evaluated DOD's efforts to implement the six pilot program requirements.

To address the second objective, we conducted structured interviews with DOD officials from across the department who are responsible for the development and management of OSS. These officials included representatives from the Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the DOD CIO, Offices of the Navy and Marine Corps CIOs, Army Communications-Electronics Command, the Defense Information Systems Agency, the Defense Advanced

[3]Pub. L. No. 115-91, § 875, 131 Stat. 1283, 1503 (Dec. 12, 2017).

Research Projects Agency, and Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics.

We obtained their views on the benefits and concerns regarding the general use of OSS. We also obtained their views on the specific requirements about the implementation of an OSS pilot program contained in OMB's memorandum. See appendix I for a more detailed discussion of our objectives, scope, and methodology.

We conducted this performance audit from August 2018 to September 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

OSS is software distributed under a license that provides broad rights to use, modify, and redistribute the original source code. Open source licenses impose certain obligations on users who exercise these rights. Specific obligations vary among the many different open source licenses. Common obligations include making the source code available, publishing a copyright notice, or giving any recipient of the program a copy of the license. Certain restrictive open source licenses allow users to copy, modify and distribute software provided that modified versions (i.e., derivatives) are subject to the same license terms and conditions as the original code. This is intended to prevent software that is derived from or contains code issued under such a license from becoming a closed-source product that can be marketed and sold exclusively.

The reuse of OSS is viewed as a promising means to reduce development costs while improving software quality. According to software experts,[4] software reuse has the potential to:

- increase reliability because systems will be developed with thoroughly tested and proven components,

[4]GAO, *Software Reuse: Major Issues Need to Be Resolved Before Benefits Can Be Achieved,* GAO/IMTEC-93-16 (Washington, D.C.: Jan. 28, 1993).

- increase productivity by reducing the time and effort needed to develop software,
- reduce costs by enabling the sharing of knowledge and practices needed to develop and maintain software, and
- establish a more standard and consistent approach to software development and maintenance by using common components and procedures.

OMB Memorandum on Federal Source Code Policy

In August 2016, OMB issued a memorandum to the heads of departments and agencies to ensure that new custom-developed source code be made available for reuse across the federal government.[5] The memorandum was intended to improve the way federal agencies buy, build, and deliver information technology and software, and required that all agencies establish a pilot program under which at least 20 percent of new custom-developed code would be released as OSS for 3 years. OMB also required that agencies develop a metric to calculate the percentage of code released as OSS to gauge its progress on implementing the pilot program.[6]

OMB's memorandum also identified four supporting requirements, among others, needed to implement an OSS pilot program:

- Issue an OSS policy that ensures code is available for government-wide reuse.
- Conduct an OSS three-step software solutions analysis that includes: (1) a strategic analysis and analysis of alternatives, (2) consideration of existing commercial solutions, and (3) consideration of custom development. In addition, agencies must consider several factors throughout each of the three-steps of the analysis such as cloud computing and open standards.

[5]OMB, *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software M-16-21* (Washington, D.C.: Aug. 8, 2016).

[6]Agencies are expected to calculate the percentage of source code released using a consistent measure—such as real or estimated lines of code, number of self-contained modules, or cost—that meets the intended objective of this requirement.

- Secure data rights to government-wide reuse and inventory new custom code, in accordance with the guidance provided by the code.gov website.[7]
- Facilitate the OSS community by developing and releasing the code in a manner that (1) fosters communities around shared challenges; (2) improves the ability of the OSS community to provide feedback on, and make contributions to, the source code; and (3) encourages federal employees and contractors to contribute back to the broader OSS community by adding value to existing projects. In doing so, agencies should comply with the following principles: (1) leverage existing communities, (2) engage in open development, (3) adopt a regular release schedule, (4) consider code contributions, and (5) document source code to facilitate use and adoption.

DOD Implementation of OMB's Open Source Software Requirements

DOD's CIO is responsible for implementing OMB's requirements for the department's OSS pilot program. The CIO reports directly to the Secretary of Defense, and is responsible for the department's information technology (including national security systems and defense business systems), information resources management, and efficiencies. The CIO is also responsible for developing strategies and policy on the operation and protection of all of the department's information technology and information systems. Other responsibilities include maintaining a consolidated inventory of mission critical and mission essential information systems, evaluating and monitoring performance measurements, and other duties to manage the information environment throughout the department.

In addition, the Defense Digital Service is responsible for assisting the CIO in implementing the OSS pilot program, among other initiatives. The Defense Digital Service is composed of commercially experienced software developers, software designers, product managers, and problem

[7]Code.gov is a website designed to help federal agencies understand what is required by OMB memorandum M-16-21. The website also shows each agency's compliance with implementing the policy. Agencies are evaluated on whether they have completed three tasks: (1) updated agency policy consistent with OMB's memorandum, (2) completed code inventory of all new custom code created after August 2016, and (3) completed open source objective to make at least 20 percent of all new custom code created after August 2016 available.

solvers within DOD. The organization works on specific projects or programs in support of the DOD in a hands-on way to materially improve digital services across the department. The Defense Digital Service also works with the CIO to monitor the identified programs, facilitate the process to open source the code, and populate the source code inventory located on Code.mil.

DOD's Efforts to Increase Use of Open Source Software

In June 2018, DOD's CIO issued a report to Congress[8] as directed by section 875(b) of National Defense Authorization Act for Fiscal Year 2018 (Public Law 115-91). The report provided Congress with the department's plan to implement the OSS pilot program established by OMB's memorandum. In the report, the CIO committed to sharing its unclassified, custom-developed source code as widely as possible in four ways: (1) review and select software programs that have self-identified to the Defense Digital Service as ready to open source its code; (2) query its contracts database to identify contracts that contain appropriate data rights language; (3) determine if source contained within existing source code repositories can be made available; and (4) issue a department-wide data call to identify and select programs where new, custom code is being developed.

The CIO also reported that the department would prioritize and assess identified software programs and work with components to develop mechanisms to report progress. The report included selection criteria for identifying candidate software programs: (1) programs with contractually secured government data rights; (2) programs with contractual rights to enable, support, and enforce DOD and government-wide sharing and reuse of custom-developed code; (3) programs that have appropriate administration to ensure that government's rights are maintained; and (4) programs that utilize best practices to ensure custom-developed code, documentation, and other associated materials are delivered in a reusable manner.

The CIO also reported that the Defense Digital Service would assist programs. Specifically, the Defense Digital Service is to develop

[8]Reports were sent to the Senate Armed Services Committee, House Armed Services Committee, Senate Appropriations Committee, and House Appropriations Committee.

guidelines, processes, and answers to frequently asked questions regarding the use of OSS.

In October 2018, the CIO issued a memorandum to the Chief Management Officer, secretaries of the military departments, Chairman of the Joint Chiefs of Staff, under secretaries of Defense, chiefs of the military services, general counsel, Director of Cost Assessment and Program Evaluation, Director of Operational Test and Evaluation, and the Assistant Secretary of Defense for Legislative Affairs notifying them of the need to implement an OSS pilot program in accordance with OMB's 2016 memorandum. The CIO required these organizations to take four actions within 30 days of issuing the memorandum:

- Identify all unclassified custom-developed source code created or paid for by the department—regardless of data rights and open source status—created on or after August 2016 and provide the CIO information required by the guidelines on the code.gov website;
- Identify and provide a point of contact that can participate in open source efforts;
- Direct authorizing officials to rapidly review and approve unclassified code for public, open source release after appropriate security, code, and policy review; and
- Direct contracting officers to secure the least restrictive data rights to custom-developed source code in all future contracts in accordance with DOD federal acquisition regulations.

DOD Has Not Fully Implemented an Open Source Software Pilot Program and Related OMB Requirements

DOD was mandated by law to initiate the OSS pilot program established by OMB memorandum M-16-21 which required (1) releasing at least 20 percent of newly custom-developed code each year for the term of the pilot program, and (2) collecting additional data concerning new custom software to inform measures to gauge the performance of the pilot program. Further, the OMB memorandum also required DOD to (1) issue an OSS policy, (2) conduct an OSS analysis, (3) secure data rights and inventory custom code, and (4) facilitate the OSS community.

As of late April 2019, DOD had not fully implemented the OSS pilot program mandated by law. DOD had partially implemented the requirement of releasing at least 20 percent of newly custom-developed code as OSS. Specifically, as of July 2019, the Code.gov website reported that the department had released less than 10 percent of its custom developed code. The department was in the early stages of its pilot program and had not determined when the pilot would be fully implemented. The CIO reported that the size of the department makes it nearly impossible to inventory all of its source code custom developed since August 2016. As such, the CIO stated that it would be difficult to meet the OMB memorandum's goal of releasing at least 20 percent of its new custom code as OSS.

In addition, DOD had not implemented the requirement to develop a consistent measure to gauge the performance of the department's pilot program. DOD had not developed such a measure due to a lack of consensus in the department about what data should be collected. According to the CIO, if the measure is "lines of code," then it unfairly discounts projects that invest a significant amount on research, but are small otherwise. If the measure is "project hours," then it discounts those projects that came about from sparks of innovation that took little time to develop. If the measure is "project count," then it ignores the other two possible measures. The CIO noted that since the components will be expected to collect and report the required data, the CIO office plans to reach out to them to facilitate consensus around data needs and what measure should be used to calculate and monitor performance.

Regarding the four OMB memorandum requirements supporting the implementation of the pilot program, the department partially implemented three and did not implement the remaining one. Table 1 describes the extent to which DOD implemented the OMB supporting requirements, and is followed by a description of DOD's efforts on each requirement.

Table 1: Department of Defense's (DOD) Implementation of Selected Supporting Requirements for Establishing an Open Source Software (OSS) Pilot Program

OMB requirement	Extent to which DOD has implemented the requirement
Issue OSS policy	Not implemented
Conduct OSS analysis	Partially implemented
Secure data rights and inventory new custom code	Partially implemented
Facilitate OSS community	Partially implemented

Key: Partially implemented = DOD provided initial plans or actions. Not implemented = DOD did not provide evidence of plans or initiated plans or actions.

Source: GAO analysis of DOD information. | GAO-19-457

Issue OSS policy. DOD had not implemented the requirement to issue an OSS policy. According to DOD's CIO, the department has existing acquisition policies applicable to OSS, such as the 5000 series[9] and a memorandum issued in October 2009 that clarifies OSS. However, according to DOD officials, these policies are outdated and do not comply with OMB's memorandum. For example, while the department's policies indicated that programs must conduct an analysis of alternatives, trade studies, or a business case analysis prior to initiating any technology acquisition or custom code development, they did not require programs to consider the value of publishing custom code as OSS and negotiate data rights reflective of its value.

The department acknowledged that it does not have a policy that addresses the OMB memorandum's requirement. According to the CIO, the department had been slow to develop a policy because these types of changes require significant resources, coordination, and buy-in across the department that will take additional time to address.

The CIO also stated that the department plans to update its existing OSS memorandum by the end of the 2019 calendar year and issue it as policy. In particular, DOD intends to work with acquisition and program management officials to define approaches, processes, and best practices to expand software reuse. If the department effectively implements this intended step consistent with the OMB memorandum, DOD should be able to fully address this requirement.

Conduct OSS analyses. DOD had partially implemented the requirement to conduct analyses to consider alternative software solutions. According to the DOD CIO, of the three elements required by OMB for a three-step analysis, the department's current 5000 series policy addresses some of these elements. For example, as previously mentioned, the policy required programs to conduct an analysis of alternatives, trade studies, or a business case analysis prior to initiating any technology acquisition or custom code development. However, according to the CIO, DOD's policy did not require programs to consider the value of publishing custom code as OSS and negotiate data rights reflective of its value-consideration.

[9]DOD's 5000 series includes the overarching management principles and mandatory policies that govern the Defense Acquisition System.

According to the CIO, the department has plans to address gaps in its existing policy by the end of the 2019 calendar year. If the department effectively implements this intended step consistent with the OMB memorandum, DOD should be able to fully address this requirement.

Secure data rights and inventory new custom code. DOD had partially implemented this requirement by initiating the process to secure data rights for government-wide reuse and inventory its new custom code. Specifically, the October 2018 memorandum called for defense organizations to direct contracting officers to secure the least restrictive data rights for custom-developed source code in all future contracts, and identify all unclassified custom-developed source code created after August 2016. However, when we discussed this matter with DOD information technology and software officials responsible for the management of software in December 2018—2 months after the October 2018 memorandum had been issued— seven of 11 officials were unaware of the statutory mandate to initiate the pilot program in compliance with the OMB memorandum. Further, DOD has not provided a milestone for when it expects its inventory to be completed.

Facilitate OSS community. DOD had partially implemented the requirement to establish an OSS community. According to the DOD CIO's Custom Developed Source Code Data Call memorandum, dated October 2018, the DOD CIO is working with Defense Digital Service to develop guidelines and processes on when and how to open source code. In February 2017, DOD announced the launch of Code.mil, an open source initiative led by Defense Digital Service, that allows software developers around the world to collaborate on unclassified code written by federal employees in support of DOD projects. Finally, the Defense Information Systems Agency established a website (Forge.mil) where community members can collaborate on open source and DOD community source software.[10] The Forge.mil website also enables collaborative development through services such as software version control, requirements management, discussion forums and document repositories.

[10]The website is available only to U.S. military, DOD government civilians, and DOD contractors for government authorized use. Access to Forge.mil requires a valid DOD Common Access Card or an external PKI (public key infrastructure) certificate issued by an accepted federal government agency, industry partner or a DOD-approved external certificate authority with a DOD government sponsor registered with Forge.mil.

However, DOD had not yet fully engaged in open source code development, established a regular release schedule for its software code, or fully documented its source code to facilitate use and adoption department-wide. According to the CIO, the department is in the early stages of implementing the OSS pilot program and had not yet published a revision to the existing OSS policy memorandum. The CIO stated that the office plans to request collaboration and input from organizations throughout DOD for improvement initiatives and identifying specific processes and expectations for improving custom-developed software within the Department. However, DOD has not provided a milestone for when the requirements will be fully implemented and stated that achieving 100 percent compliance is not a realistic expectation.

Until DOD fully implements the OSS pilot program mandated in the National Defense Authorization Act for Fiscal Year 2018 including the requirements of OMB memorandum M-16-21, the department will likely miss opportunities to achieve related cost savings and efficiencies. Further, the department will not be effectively positioned to ensure management oversight and implementation of the pilot program.

DOD Officials Shared Views of Expected Benefits and Risks Associated with the Use of Open Source Software

DOD Officials Agree That Using Open Source Software Could Result in Financial Benefits and Increased Efficiency

DOD officials representing 11 components reported that OSS can potentially yield financial benefits and increase efficiency. Officials provided the following examples of financial benefits:

- Officials in the office of the Navy Chief Information Officer, the Army Communications-Electronics Command, the Office of the Under Secretary of Defense for Acquisition and Sustainment, and the Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics stated that OSS is generally less expensive than commercial off-the-shelf (COTS) leading to cost savings.
- An Air Force official we spoke with stated that the increased use of OSS may potentially result in cost savings. Further, the official noted

general criteria used by the Air Force to identify software projects that may potentially be appropriate for the use of OSS. Specifically, OSS should be considered if, among other things, the required maintenance would not result in a reduction of cost savings or efficiency if the maintenance is performed in-house.

- An official we spoke with at the Defense Advanced Research Projects Agency stated that OSS has positive benefits in terms of reducing costs by reducing duplicative efforts. In addition, this official also stated that OSS allows institutions of any size and budget to partake in shared investments providing access to software capabilities at a much lower cost.
- A program manager from the Defense Information Systems Agency reported that the agency had identified an OSS solution that provided more functionality at less cost than the commercial solution provided through a vendor. The program manager explained that when the agency implemented the new OSS solution, it realized $20 million in annual savings over the commercial solution that had been maintained by a vendor.

Officials also shared examples of how OSS can increase efficiency in software development. For example,

- Officials from the offices of the Navy CIO and the US Marine Corps CIO stated that OSS solutions may increase efficiency by providing a rapid resolution to the needs and requirements of users. In contrast, rapid development efforts are not conducive for COTS solutions because of the long process required to obtain solutions that are needed quickly.
- Similarly, an Air Force official noted that the increased use of OSS may result in increased efficiency by providing rapid responses to user requirements.
- A program manager from the Defense Information Systems Agency reported that the selection of an OSS solution rather than a COTS solution contracted through a vendor had resulted in increased efficiency. The official explained that the use of the OSS solution allowed the agency to develop and maintain in-house skills that would not have been available had they opted to contract with a vendor providing a skilled workforce.

DOD Officials Expressed Differing Views on the Cybersecurity Risk Posed by Open Source Software

Officials from the 11 components expressed mixed views on managing cybersecurity risks that could be posed by using OSS. Specifically, officials from three components expressed their views that security concerns and the lack of a cybersecurity governance process could result in the sporadic use of OSS. For example:

- A Navy CIO official viewed insider threats, such as a disgruntled employee embedding malicious code, as a factor that could significantly limit the use and sharing of OSS. According to Navy officials, without a process to verify that the software is free of malicious code, the Navy would risk the assurance it requires to increase the use of OSS. The official said that, in contrast, such concerns are not an issue when it comes to COTS software because of the test and verification process to ensure it is free from malicious code.
- An official in the office of the Marine Corps CIO stated that OSS is used sporadically in their software development efforts because some cybersecurity officials within the Marine Corps discourage its use due to security concerns.
- An official from the Army's Communications-Electronics Command noted that DOD lacks a governance process once the originating entity releases the source code as open source. The originating entity no longer retains control over redistributed versions of the source code. According to Communications-Electronics Command officials, Army project managers may be hesitant to utilize OSS because of this perceived security risk.

On the other hand, DOD officials from eight components stated that the potential cybersecurity risks posed by the use of OSS were manageable and that the use of OSS should not be limited. For example:

- The policy advisor from the Office of the Under Secretary of Defense for Acquisition and Sustainment noted that scanning tools to analyze and identify safe and reliable open source code are not being used. Employing available scanning tool options could result in discovering available OSS. The policy advisor also noted that building security into software operations, rather than through the development of software, would enable users to know if code has been subverted and to react appropriately.

- A program management official from the Office of the Under Secretary of Defense for Acquisition and Sustainment suggested that security concerns may be mitigated by establishing a secure repository for trusted code.
- An official in the Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics reported that, as long as OSS is properly vetted to ensure it is secure and free from malware, it offers an opportunity for the department to achieve cost savings and efficiencies.

Conclusions

Pilot testing the use of OSS is an important way to ascertain and improve the way DOD buys, builds, and delivers information technology and software solutions. However, the department is in the early stages of implementing its pilot program and had not determined when the pilot would be fully implemented. Specifically, DOD has not made 20 percent of its new code available for reuse nor has it identified a measure to gauge the performance of its pilot program. Moreover, DOD has not yet established milestones for securing data rights and conducting an inventory or facilitating community. Until DOD fully implements its pilot program and establishes milestones for completing the OMB requirements, the department will not be positioned to take advantage of significant cost savings and efficiencies.

Recommendations for Executive Action

We are making the following four recommendations to DOD:

- The Secretary of Defense should ensure the department implements the pilot program by releasing at least 20 percent of newly custom-developed code as OSS. (Recommendation 1)
- The Secretary of Defense should ensure the department identifies a measure to calculate the percentage of code released to gauge its progress on implementing the pilot program. (Recommendation 2)
- The Secretary of Defense should ensure the department establishes milestones for completing the requirements of OMB memorandum M-16-21 of securing data rights and conducting an inventory. (Recommendation 3)

- The Secretary of Defense should ensure the department establishes a milestone for completing the OMB memorandum's requirement of facilitating an OSS community. (Recommendation 4)

Agency Comments and Our Evaluation

DOD provided written comments on a draft of this report, which are reproduced in appendix II. In its comments, the department did not concur with our first recommendation, partially concurred with our second recommendation, and concurred with the third and fourth.

DOD did not concur with the first recommendation on ensuring that the department implements the pilot program by releasing at least 20 percent of newly custom-developed code as OSS. The department stated that it does not believe that the pilot program as described in the OMB memorandum is implementable as proposed. For example, DOD asserts that most of DOD's custom developed software is created for weapons systems and releasing the associated code is sensitive for national security reasons. In addition, the size and complexity of DOD presents unique challenges for the department compared to other federal agencies such as inventorying all software development projects to establish a baseline. DOD added, however, that the OMB memorandum explicitly states that national security exceptions do not apply to the pilot program. DOD also stated that it recognizes the value of collaborative software development and has plans to release additional guidance on releasing OSS and procedures for maintaining its inventory. Once DOD establishes a baseline inventory of custom-developed software and the procedures for maintaining it, the department states it will be able to determine if the 20 percent is an appropriate goal.

We understand the potential constraints DOD faces and that national security considerations are to be factored into decisions DOD will need to make about which custom developed software to include in the pilot. However, DOD is mandated by law to implement the OSS pilot program established by OMB memorandum M-16-21. Further, the OMB memorandum instructs agencies to refrain from selecting code for release that would fall under exceptions such as national security risk. As such, DOD has flexibility on making decisions about which custom-developed code to include in the pilot. While we agree that a baseline inventory is needed, DOD must include at least 20 percent of new custom-developed code each year for the term of the program to satisfy the mandate.

DOD partially concurred with the second recommendation on ensuring that the department identifies a measure to calculate the percentage of code released to gauge its progress on implementing the pilot program. Specifically, the department stated that the additional guidance it plans to release before the end of 2019 on OSS will include measures to gauge how much code has been developed and how much has been released. In addition, DOD noted that these measures will support good management of the overall portfolio of information technology, even in the absence of the mandated pilot program established by the OMB memorandum. We believe that the measure to calculate the percentage of code should be used to assist the department in meeting the OMB memorandum's requirements. We also agree with the benefits of developing a measure to manage the portfolio of information technology.

DOD concurred with the third and fourth recommendations related to establishing milestones for completing the OMB memorandum's requirements of securing data rights, conducting an inventory, and facilitating an OSS community. According to the department, it has issued a memorandum that directed contracting officers to secure the least restrictive data rights to custom-developed source code, in furtherance of the OMB requirements, and also included a data call that forms an initial basis of an inventory of custom-developed software. Regarding facilitating an OSS community, DOD stated that it has formed a community of practice called DevSecOps that is open to all software development organizations in the department and plans to use this forum to facilitate collaboration on the use of OSS.

We are sending copies of this report to the appropriate congressional requesters and the Secretary of Defense. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staffs have any questions about this report, please contact me at (202) 512-4456 or at harriscc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Carol C. Harris
Director,
Information Technology Management Issues

List of Committees

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard C. Shelby
Chairman
The Honorable Dick Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Pete Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to: (1) assess the extent to which the Department of Defense (DOD) has implemented the open source software (OSS) pilot program and other related requirements established by the Office of Management and Budget (OMB), and (2) describe the views of responsible DOD officials on the use of OSS to achieve efficiency at the department.

To address the first objective, we selected six requirements from the OMB memorandum titled the *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software* (M-16-21, Aug. 8, 2016) as criteria to assess the extent to which DOD has implemented the OSS pilot program. Two requirements establish the OSS pilot program: (1) releasing at least 20 percent of newly custom-developed code each year for the term of the pilot program, and (2) developing a metric to gauge the performance of the pilot program. The other four requirements support the implementation of the pilot program: (1) issuing an OSS policy, (2) conducting an OSS analysis, (3) securing data rights and inventorying custom code, and (4) facilitating the OSS community. We met with officials from OMB to collect background information on the selection of requirements for the pilot program established in memorandum M-16-21. We also met with officials from the Office of the DOD Chief Information Officer (CIO) and the Defense Digital Service to discuss the status of the department's implementation of the OSS pilot program.

We reviewed DOD's June 8, 2018 report to Congress and its October 2018 memorandum that details the department's plans to implement the pilot program and compared them to the six requirements. To determine the extent to which the pilot program had been implemented, we evaluated DOD's efforts to address each of the requirements using a 3-stage gradient scale (implemented, partially implemented, and not implemented). The requirement was assessed to be fully implemented if DOD provided us with sufficient evidence that the requirement had been fully met. We assessed a requirement to be partially implemented if DOD provided us with documentation of initial plans or had initiated action towards implementing the requirement. We determined that a

requirement was not implemented when DOD did not provide us with documentation of planned or initiated actions to implement the requirement.

To address the second objective on views of various responsible DOD officials, using professional judgement, we selected components across the department responsible for the management and development of OSS. The scope of stakeholders selected represent department-wide nongeneralizable views including military components, defense agencies, and other offices. At least one representative was selected from the following components: (1) Office of the Under Secretary of Defense for Acquisition and Sustainment, (2) Office of the DOD CIO, (3) office of a military service CIO, (4) Military Service Software Center or Command Center, (5) the Defense Information Systems Agency, and (6) the Defense Advanced Research Projects Agency. We conducted interviews with DOD officials from the following entities: Office of the Under Secretary of Defense for Acquisition and Sustainment; Office of the DOD CIO; Offices of the Navy and Marine Corps CIOs; Office of the Air Force Chief Technology Officer; Army Communications Electronics Command; the Defense Information Systems Agency; the Defense Advanced Research Projects Agency; and the Office of the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics.

In order to summarize and report the views of the responsible DOD officials, we conducted structured interviews with representatives from the selected components. Each interview consisted of the same discussion topics based on the pilot program requirements established in OMB's memorandum. The scope of this objective represents individual thoughts, views, and opinions and is not intended to convey an official or department response.

Prior to each interview, participants were provided with OSS discussion topics, and the OMB memorandum, titled the *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software* (M-16-21, Aug. 8, 2016). The contents of each interview were reviewed and summarized to identify the general views of OSS and on the anticipated implementation of the pilot program requirements established in OMB's memorandum. We noted similarities and differences in the responses provided by the officials in the use of OSS including, but not limited to, potential benefits of using OSS, managing associated risk, and opinions on implementing the pilot program in compliance with the OMB memorandum.

Discussions were split into two topic areas: practices on the use of OSS, and OMB's memorandum to establish an OSS pilot program. Specifically, the discussion topics were presented during each meeting as follows:

Part I: Practices on the use of OSS

- Your experience or your organization's history with the practice of using OSS as a means to achieve cost reduction or efficiencies when buying, building, or delivering information technology and software solutions.
- The processes or practices that you or your organization perform to leverage open source code for projects that require the acquisition or development of custom source code.
- The extent to which you or your organization shares or uses open source software. For example, do you share or use open source software: (1) within your organization only, (2) across the DOD with other military services or defense agencies, (3) with other federal agencies, or (4) outside the federal government with the public. Also, how is the source code shared, leveraged, catalogued, stored, and accessed.
- Policies or guidance currently in use for OSS.
- General views and opinions on the use of open source code.

Part II: OMB's Memorandum to Establish an OSS Pilot Program

- When and how you or your organization became aware of OMB's memorandum on Federal Source Code Policy.
- Your opinions and views about the OMB memorandum.
- Any specific concerns or reservations about the requirements contained in the OMB memorandum.
- The extent to which you or your organization may already be performing the steps in OMB's proposed Three-Step Software Solutions Analysis.
- Discuss the feasibility of the pilot program requirement to release at least 20 percent of new custom-developed code as OSS.

We conducted this performance audit from August 2018 to September 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Defense

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

JUL - 3 2019

Ms. Carol C. Harris
Director, Information Technology
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

This is the Department of Defense (DoD) enclosed response to the GAO Draft Final Report, GAO-19-457, 'INFORMATION TECHNOLOGY: DOD Needs to Fully Implement Program for Piloting Open Source Software,' dated May, 2019 (GAO Code 102984).

The Department appreciates the opportunity to review the final report. My point of contact for this matter is Mr. Daniel Risacher, daniel.r.risacher.civ@mail.mil, (571) 402-5275.

Sincerely,

for Dana Deasy

Enclosure:
As stated

GAO DRAFT FINAL REPORT DATED MAY 1, 2019
GAO-19-457 (GAO CODE 102984)

"INFORMATION TECHNOLOGY: DOD NEEDS TO FULLY IMPLEMENT PROGRAM FOR PILOTING OPEN SOURCE SOFTWARE"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the department implements the pilot program by releasing at least 20 percent of newly custom-developed code as OSS.

DoD RESPONSE: Nonconcur. The Department recognizes the value of collaborative software development, and agrees with the establishment of policies and processes to release custom-software as open-source within reasonable constraints. The Department does not believe that the OSS pilot program described by OMB Memorandum M-16-21 is implementable by the Department of Defense as proposed. In particular, OMB Memorandum M-16-21 recognizes necessary exceptions to government code reuse for national security reasons, but explicitly states that these exceptions do not apply to the proposed OSS Pilot. Most of the Department's custom-developed software is created for weapons systems like the F-35 and F-22, and as such, release of such source code is sensitive for national security reasons and is typically restricted by arms-control regulations. Given these constraints, it is unclear that twenty percent of the Department's custom-developed code is releasable at all.

Furthermore, the size and complexity of the Department of Defense presents unique challenges for inventorying all software development projects, compared to other federal agencies. In order to meet any target percentage, the Department will first need to establish a baseline inventory of software development activities, as well as the processes to maintain that inventory over time. Once this is accomplished, the Department will be able to determine if twenty percent is an appropriate goal.

The DoD CIO, in conjunction with the Office of the Undersecretary of Defense for Acquisition and Sustainment, is in the process of developing policy concerning the development of custom-developed software, which will include procedures for maintaining an inventory of custom-developed code, and additional guidance on releasing such code as OSS. The CIO anticipates this guidance being issued before the end of 2019.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the department identifies a measure to calculate the percentage of code released to gauge its progress on implementing the pilot program.

DoD RESPONSE: Partial concur. The policy and guidance described above will include measures to gauge how much code has been developed and how much has been released. These measures will support good management of the overall portfolio of information technology, even if the Department does not implement the specific pilot as described in M-16-21.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure that the department establishes milestones for completing the OMB requirements of securing data rights and conducting an inventory.

DoD RESPONSE: Concur. The DoD CIO has already issued a memorandum that directed that contracting officers secure the least restrictive data rights to custom-developed source code, in furtherance of the OMB requirements, and also included a data call that forms an initial basis of the DoD's inventory of custom-developed software. This initial inventory is incomplete, for reasons described above. The forthcoming guidance will be issued in 2019, and will establish procedures for updating this inventory and will establish additional milestones.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that the department establishes a milestone for completing the OMB requirement of facilitating an OSS community.

DoD RESPONSE: Concur. The DoD CIO has formed a DevSecOps Community of Practice that is open to all software development organizations in the DoD, and will use this forum to facilitate OSS and OSS methodologies. While the initial meetings of this community have not addressed OSS-specific issues, these will be part of the community agenda by 4QFY19.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, (202) 512-4456 or harriscc@gao.gov

Staff Acknowledgments

In addition to the contact named above, Eric Winter (Assistant Director), John Ortiz (Analyst-in-Charge), Rebecca Eyler, Franklin Jackson, and Kate Nielsen made key contributions to this report.

Appendix IV: Accessible Data

Agency Comment Letter

Accessible Text for Appendix II Comments from the Department of Defense.

Page 1

JUL - 3 2019

Ms. Carol C. Harris

Director, Information Technology

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Dear Ms. Harris:

This is the Department of Defense (DoD) enclosed response to the GAO Draft Final Report, GAO-19-457, 'INFORMATION TECHNOLOGY: DOD Needs to Fully Implement Program for Piloting Open Source Software,' dated May, 2019 (GAO Code 102984).

The Department appreciates the opportunity to review the final report. My point of contact for this matter is Mr. Daniel Risacher, daniel.r.risacher.civ@mail.mil, (571) 402-5275.

Sincerely,

Essye B. MIller

for Dana Deasy

Enclosure:

As stated

Page 2

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the department implements the pilot program by releasing at least 20 percent of newly custom-developed code as OSS.

DoD RESPONSE: Nonconcur. The Department recognizes the value of collaborative software development, and agrees with the establishment of policies and processes to release custom- software as open-source within reasonable constraints. The Department does not believe that the OSS pilot program described by 0MB Memorandum M-16-21 is implementable by the Department of Defense as proposed. In particular, 0MB Memorandum M-16-21 recognizes necessary exceptions to government code reuse for national security reasons, but explicitly states that these exceptions do not apply to the proposed OSS Pilot. Most of the Department's custom- developed software is created for weapons systems like the F-35 and F-22, and as such, release of such source code is sensitive for national security reasons and is typically restricted by arms- control regulations. Given these constraints, it is unclear that twenty percent of the Department's custom-developed code is releasable at all.

Furthermore, the size and complexity of the Department of Defense presents unique challenges for inventorying all software development projects, compared to other federal agencies. In order to meet any target percentage, the Department will first need to establish a baseline inventory of software development activities, as well as the processes to maintain that inventory over time. Once this is accomplished, the Department will be able to determine if twenty percent is an appropriate goal.

The DoD CIO, in conjunction with the Office of the Undersecretary of Defense for Acquisition and Sustainment, is in the process of developing policy concerning the development of custom- developed software, which will include procedures for maintaining an inventory of custom- developed code, and additional guidance on releasing such code as OSS. The CIO anticipates this guidance being issued before the end of 2019.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the department identifies a measure to

calculate the percentage of code released to gauge its progress on implementing the pilot program.

DoD RESPONSE: Partial concur. The policy and guidance described above will include measures to gauge how much code has been developed and how much has been released. These measures will support good management of the overall portfolio of information technology, even if the Department does not implement the specific pilot as described in M-16-21.

Page 3

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure that the department establishes milestones for completing the OMB requirements of securing data rights and conducting an inventory.

DoD RESPONSE: Concur. The DoD CIO has already issued a memorandum that directed that contracting officers secure the least restrictive data rights to custom-developed source code, in furtherance of the 0MB requirements, and also included a data call that forms an initial basis of the DoD's inventory of custom-developed software. This initial inventory is incomplete, for reasons described above. The forthcoming guidance will be issued in 2019, and will establish procedures for updating this inventory and will establish additional milestones.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that the department establishes a milestone for completing the 0MB requirement of facilitating an OSS community.

DoD RESPONSE: Concur. The DoD CIO has formed a DevSecOps Community of Practice that is open to all software development organizations in the DoD, and will use this forum to facilitate OSS and OSS methodologies. While the initial meetings of this community have not addressed OSS-specific issues, these will be part of the community agenda by 4QFY19.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548