FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

Why feds shouldn't fear GitHub

By Derek B. Johnson
Feb 21, 2020

https://fcw.com/articles/2020/02/21/open-source-feds-johnson.aspx

For years, the software development community has tried to push back on fears that open-source development tools are inherently less secure. In the federal government, they're still having the debate, but federal IT leaders are increasingly making the same argument.

During a Feb. 20 event hosted by the American Council for Technology and Industry Advisory Council, U.S. Citizenship and Immigration Services Deputy CIO Yemi Oshinnaiye said IT leaders are slowing learning how to build an effective software development culture in government projects. Part of that evolution is using the best tool for the job.

He recounted one project where his team needed to process a change request for a router that shared an enterprise environment with the Secret Service and Transportation Security Administration. Oshinnaiye wanted a quick way for his development, infrastructure and security teams to keep tabs on each other's work. He suggested they use GitHub, an open-source software development platform.

"'You can't use GitHub, that's a public tool! You can't do it, it has no security!'" He recalled hearing from skeptics on the project. "Really? It's a public tool with people that work on it [all the time], it has more security than the things that we're using internally."

For years, open-source software has been met with suspicion by some developers, who point to examples like the Equifax hack, which took advantage of vulnerabilities found in Apache Struts software and the Heartbleed bug, which exploited OpenSSL's encryption library, as prime examples of insecurity in many public tools. A recent study by the Linux Foundation found that 80% to 90% of any modern piece of software is composed of open-source code. This same proliferation and reuse means there is no central authority to conduct quality control or keep track of when code is altered, potentially introducing new vulnerabilities.
According to Oshinnaiye, it took time to convince his colleagues that they weren't putting their projects at risk by leveraging what was already publicly available on the internet.

"It was a fight. It wasn't easy, I think it took about a year and some change, but then we said we're starting to use GitHub," he said. "Now I have a repository where I'm going to

put scripts for infrastructure, scripts for development and scripts for security in one place. Now that's revolutionary. It's very simple, but it's revolutionary."

When asked by FCW what conditions were necessary to make developers feel comfortable using open-source tools, several other feds echoed Oshinnaiye's outlook.

"We're open source for the way we develop, and the Smithsonian actually has a GitHub account … so if your enterprise adopts it, that's like the No. 1 great thing," said Ravyn Manuel, a senior application developer and DevOps engineer for the Smithsonian National Museum of African American History and Culture. "And then for the tools, open source is free, so it's really cost effective."

Agencies like the Office of Management and Budget believe that federal agencies should not only use open-source code where possible, they should contribute to it when they can. Since 2016, OMB has required civilian agencies to release up to 20% of their custom code to Code.gov, where anyone can use it.

Not everyone in the federal government feels the same way. The Department of Defense has not issued an open-source policy, and CIO Dana Deasy told auditors last year that most of DOD's custom software is "sensitive for national security" and made for weapons systems like the F-35 and the F-22. Deasy said it's "unclear that 20% of the Department's custom code is releasable at all."

"I really strongly believe in [open source], and I hope that everybody here posts their code when it's possible," said William Daus, branch chief for National Science Foundation's research directorate. "I know that sometimes it's not, but it is good to share and reuse."