Q&A

Executive Viewpoint

A conversation with the Air Force about open source

Lauren Knausenberger
CIO, Air Force

Lt. Col. Brian Viola
Materiel Leader,
Platform One, Air Force

Maj. Camdon Cady
CTO, Platform One,
Air Force

Why are you so enthusiastic about open source?

Knausenberger: Open source is the foundation of most of the world's software. And if you look at the top 10 open source contributors in the world, you'll see a lot of household names like Microsoft and Google. Companies that we trust and buy from in large dollar amounts in the Department of Defense are largely the folks who are contributing to open source software.

Then we look at how much the hearts and minds in DOD are willing to adopt something. A number of years ago, folks were still a little skittish about open source, but we now have policies saying free and open source software is trusted and something we want to adopt within the DOD.

We've also shown that we can use open source. Platform One has been a huge part of our success in leveraging open source software, and it means we get to use great software without necessarily paying for the same code over and over. In addition, open source is inherently more secure because the eyes of the crowd are looking at it. All of that comes together to make me pretty bullish on open source.

Viola: I'll just add that open source involves both consuming and contributing, and with the evolution of policy, the DOD now promotes that bidirectional flow. At Platform One, we fully participate in the open source community, both consuming and contributing back fixes and enhancements.

Cady: We do regular evaluation and testing of software at Platform One, and we've had several cases now where we found something and were able to fix it and contribute that fix back to the community. If something's a high priority for us, we can directly contribute that back, and everyone benefits from it. When other people contribute to open source software, we reap those same benefits.

How does the Air Force support the use of open source technology to achieve its mission goals?

Viola: At Platform One, we deliver a tailorable tech stack for continuous integration and continuous delivery of warfighter capabilities. We do that through four primary lines of effort we call value streams. Big Bang is platform services, tailorable to mission need. Iron Bank really ups the game on supply chain security, seeking out and eliminating attack vectors. The Cloud Native Access Point is a zero trust way to bring single sign-on across multiple impact or classification levels. Finally, Party Bus serves up all those capabilities as a service to DOD organizations.

For each capability in the Big Bang tech stack, users can select from an open source and a paid component, which comes with the advanced support that vendors provide.

Cady: About two-thirds of the software on Iron Bank — about 700 pieces — is listed as open source, and the most popular packages tend to be open source.

How does open source fit into your efforts to ensure secure agile software development?

Knausenberger: Our top-performing teams use agile software development practices, and the vast majority of those high-performing teams also leverage open source. As much as open source software is inherently more secure, there are some areas where we do not use it. We need the ability to add that special

> **We now have policies saying free and open source software** is trusted and something we want to adopt within the DOD."

sauce that gives us our competitive advantage as a military organization. Again, this is where tools like Iron Bank come into play because we can reuse containers.

Cady: We validate the identities of anyone who wants to bring a piece of software into Iron Bank and then we apply fairly strict standards about how the software is packaged. One of the more unique things we've done since the beginning, and now the commercial world is starting to do as a paid service, is to constantly rebuild the containers on Iron Bank and then rescan them. As a result, we can pull in updates from every level quickly, which helps us deal with things like the Log4j vulnerability a lot faster than some other systems can.

We're never going to write software that has no flaws or is perfectly configured. So we want to be able to react very quickly when something is discovered, and that starts with awareness of what you have so that when something like Log4j drops, you can fix it.

Viola: We have commercial organizations that are using Iron Bank containers because it adds a layer of security to open source products beyond downloading them off the internet. However, you're never done with security. The adversary will adapt and find new attack vectors, so at Iron Bank, we are looking to continuously make it more difficult for the adversary. To be clear, this is not just about open source products. It's about commercial products and the dependencies between commercial and open source products.

What role do you see for vendor-supported open source technology in government?

Knausenberger: Within Platform One, we have a pure open source option that a great team of people helped us build. We also have some vendor-specific stacks. In each case, the intent is for a development team to be able to have the tools they need to start coding in terms of leveraging open-source tools and libraries and also in terms of not having to handle the integration and spin-up of the stack.

Because we don't have thousands of software developers, we have vendor partners help us deploy our platforms to get the most out of our open-source software, coding side by side with us. That's part of how we continue to cross-pollinate and make sure that we can bring commercial best practices into government.

What advice do you have for other agencies that want to adopt or expand their use of open source?

Cady: Organizations like the Open Source Security Foundation and the National Institute of Standards and Technology have done a lot of work to provide frameworks for making decisions about open-source software. Stand on the shoulders of giants and use those frameworks. If you want to get contributions to your open-source project, be as clear as possible about who can contribute and how they can contribute. There are a lot of people who want to help, but they need to know how to do it.

Knausenberger: You have to have the institutional will to use open source. You may have folks in the organization who aren't tracking that the entire world is using open source. Seeing how important open source is can help organizations that might be a little behind culturally.

But it really comes down to this: Open source will help with agility and security, but you have to have a team that knows what it's doing. An open source project is inherently more secure if a lot of smart people have looked at it, identified vulnerabilities and fixed them. If a project is stale and the only developers are in China, maybe you shouldn't use it. We have incredibly talented employees. We have to empower them, put them in charge and let them figure it out.

It's also really important to find the right industry partner. You can't go from a hardware company to a software company overnight within government bureaucracies, unfortunately, so you have to partner through that transition. ■

Leverage open source innovation with the built-in security, scalability and support required in public sector IT.

The open source development model ensures constant innovation and iteration through a decentralized community of thousands of contributors to projects' codebases. Enterprise open source software providers leverage the innovation of community-driven open source projects, while embedding the built-in security, scalability and support required in the enterprise environments of public sector IT organizations.

Red Hat	ACQUIA	Alfresco	ANACONDA
anchore	CloudBees	CLOUDERA	Cockroach Labs
Coder	CONFLUENT	Couchbase	databricks
elastic	EDB POWER TO POSTGRES	ForgeRock	GitLab
HashiCorp	H2O.ai	KEYFACTOR	Liferay
Liquibase	Lucidworks	redis	rocket.chat
MariaDB	Mattermost	MongoDB	neo4j
solo.io	sonatype	Starburst	TIDELIFT

Carahsoft provides Federal, State and Local Government agencies as well as Education and Healthcare organizations with enterprise open source software solutions to modernize their approach to IT. Visit carah.io/OpenSource to learn more about Carahsoft's industry-leading portfolio of enterprise open source software providers and identify the most suitable solution for your agency's IT needs.

carahsoft

The Trusted Government
IT Solutions Provider®