# Balancing speed and security with SecDevOps

By adapting how the government builds software, systems can be more open, flexible and secure

**Paul Burnette**
Leidos

THE FEDERAL government operates some of the most sensitive networks and systems in the world. As demonstrated by the impact of recent high-profile cyberattacks, deploying less-than-optimal code on those systems opens the doors to potential adversaries and has ripple effects across our economy and our daily lives.

Code used to be built and run on a server behind a locked door. However, the unprecedented modernization the government is undergoing has the unintended consequence of making software more vulnerable given the wide range of contributors and technologies involved in building and operating the components of that software. As a result, there are more surfaces to attack and it has become more difficult to secure crucial government systems.

It is critical that government and industry work together to develop and deploy hardened, optimal code in everything we do.

## ADDRESSING THE ENTIRE LIFE CYCLE OF SOFTWARE

Agile development and delivery, while paramount, cannot come at the expense of security. At Leidos, we believe security isn't a checkbox exercise after software is built. The only way to overachieve on security is to make it first and central to everything we do. That's why we say SecDevOps instead of DevSecOps.

That approach gives us the ability to rapidly and reliably deploy software, operate it and understand how it's working so that we can enhance and update it in a secure way. In other words, we're not just pushing out new software. We are refactoring and maintaining software while proactively adjusting our security posture because adversaries never stop trying to get in. They're constantly evolving, and our software has to evolve and outpace those threats.

> "**It is critical that government and industry work together** to develop and deploy hardened, optimal code in everything we do."

In addition, reusing successful code lets us move faster and focus on solving new or emerging problems. However, we need to make sure all the elements we're using are secure. At Leidos, we work closely with our technology partners so we can present holistic security solutions to our customers, particularly for sensitive government systems.

## LEADING-EDGE SOLUTIONS THAT EVOLVE AT MISSION PACE

As one of the largest systems integrators, Leidos understands the government's mission domain and individual agencies' unique challenges. We also know where they are in their evolution. Some are still easing toward agile and SecDevOps, whereas others have fully embraced those approaches.

Our partners in the commercial world are some of the fastest, most forward-leaning technologists. For example, HashiCorp has built a capability focused on infrastructure as code — software that helps define and manage IT environments in an effective, efficient way. The ability to use code to manage the infrastructure on which


software is deployed and operates is a valuable component of our SecDevOps approach.

HashiCorp's Terraform enables infrastructure creation from the ground up, and the company's Vault gives us the ability to dynamically secure different pieces of software using secrets and keys that can only be paired together by the right people.

Through partnerships like this, Leidos combines emerging technologies with our expertise in government missions to move faster and customize capabilities to specific situations. As a result, we make it easier for agencies to implement leading-edge, secure solutions that evolve at mission pace. ■

**Paul Burnette** is vice president and director of the Software Accelerator at Leidos.