GovCIO MEDIA & RESEARCH

JUNE 2026

DeepDives

THE RISE OF PLATFORM ENGINEERING in GOVERNMENT

INSIDE:

SPONSORED BY

CDW

From the editor's desk

Sarah Sybert, Managing Editor

Software at Speed and Scale

Software is central to nearly every government mission, forcing agencies to rethink how applications are developed, secured and delivered to operational environments.

Across the War Department, leaders are advancing DevSecOps and platform engineering strategies to shorten deployment timelines, automate security processes and reduce the friction that has historically slowed software modernization. Agencies are moving away from disconnected development environments and manual authorization and toward standardized platforms that integrate infrastructure, security and deployment into a continuous process.

Officials say this shift is helping agencies move closer to a "production as a service" model, where developers spend less time managing infrastructure and compliance requirements and more time building mission capabilities.

Generative AI also is influencing the software development lifecycle. Agencies are exploring how AI can automate tasks for coding, testing and documentation to improve productivity and accelerate modernization efforts. That evolution is also raising new questions around governance, cybersecurity and oversight of these AI-enabled tools.

The goal is to create resilient, repeatable and secure software ecosystems capable of adapting to rapidly changing mission needs. As agencies push to modernize legacy systems and deploy capabilities faster, DevSecOps and platform engineering are key pieces of the government's next phase of digital transformation.

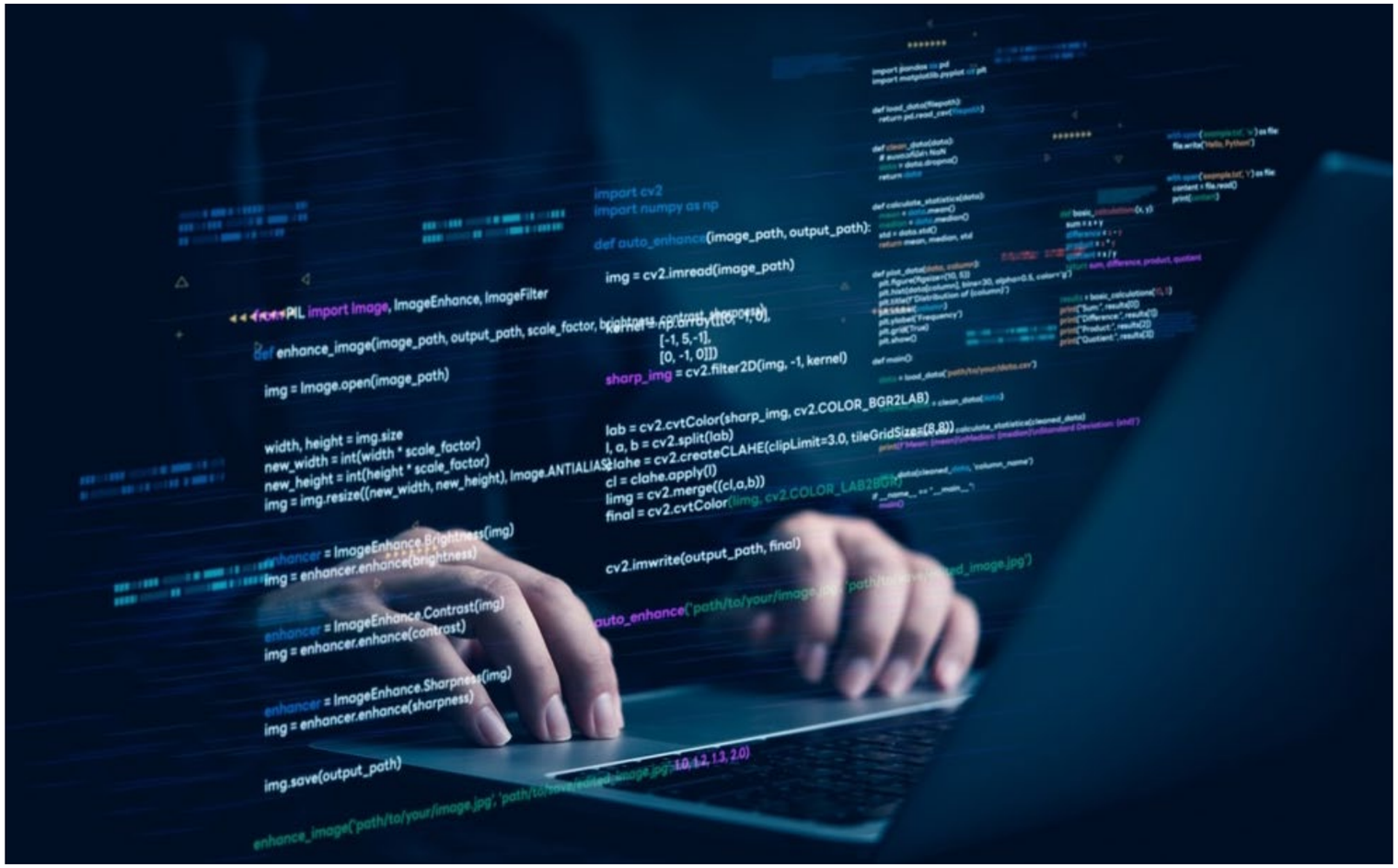
Table of Contents

Ross Gianfortune, Senior Staff Writer

Platform Engineering Pushes Government to 'Production as a Service'

Marine Corps' Operation StormBreaker reduces developer burden, automates risk management framework controls and accelerates secure code delivery into production.

BY ROSS GIANFORTUNE



Government agencies and defense contractors are adopting platform engineering to accelerate software deployment and reduce delays, noted Marine Corps Community Services Chief Digital Business Officer David Raley.

The model shifts away from manual authorization processes toward centralized platforms where infrastructure and security are delivered as a service, reducing the technical overhead required to achieve an authority to operate (ATO). Raley's team is demonstrating this approach with Operation StormBreaker, a program aimed at tackling slow development cycles and burdensome authorization processes.

"We endeavor to abstract away almost all of the underlying infrastructure complexity from the engineer and focus them only on the application layer," Raley said. "That's what we do. And we provide the platform capability to the vendor or the mission owner, or on behalf of the mission or to the vendor, right to the application team as a service."

Abstracting the Complexity

As the Pentagon confronts increasingly software-defined missions, the War Department is emphasizing a shift toward standardized development platforms.

DOW's 2023 Digital Engineering Strategy called for establishing policy for platform engineering across acquisition programs and for a department-wide integrated digital approach that emphasizes digital engineering environments

Photo credit: khunkornStudio/Shutterstock

must enable earlier testing, faster iteration and more resilient software.

Then in January, the department's Digital Standards Strategy adopted additional procedures for platform engineering. The strategy referenced standards from the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

"This allows for end-to-end online standards development and configuration management processes. With this, ISO/IEC is also exploring the business models for distributing and commercializing SMART standards and identifying related legal implications in a newly digital market," the Defense Standardization Program Office wrote in the strategy.

The department has a series of platform engineering initiatives within its DevSecOps ecosystem, including the flagship Platform One, according to officials.

"The best example is Platform One," George Lamb, director of DOW's Cloud and Software Modernization, told GovCIO Media & Research in 2025. "Working hand-in-hand with how we built Platform One, [the platform engineering ecosystem incorporates] Kubernetes, the containers, the service mesh and the way that microsegmentation and zero trust are built in."

Reducing Cognitive Load

The goal of StormBreaker and similar platform engineering initiatives is to reduce the "cognitive load" on developers. In a traditional government setting, a software engineer isn't just writing code, but also navigating Kubernetes configurations, network pathing and complex risk management Framework (RMF) documentation.

"The issue is of a little wider scope than the cognitive load on platform engineers," Raley said. "It's all of the underlying infrastructure, the security control inheritance, the deeper look from a cybersecurity perspective and the way that you can position engineers to build and deploy code securely in minutes, as opposed to them focusing on all the other things."

(ctd.)

Raley said production — not sandbox environments — must serve as the "north star" for development. He described Operation StormBreaker as a "production-as-a-service" platform, designed to enable rapid deployment by decoupling infrastructure from application logic.

"[Sandbox overuse] is a problem that has plagued some of the software platforms across the DOW," Raley said. "Most of them end up being in kind of 'research, repair and treat it' ... StormBreaker's north star has always been production. We know that that's where the real impact is."

Shifting Cybersecurity Outcomes

Raley said that platform engineering excels in its the ability to "shift left" on cybersecurity. Instead of waiting months for a final audit, developers receive real-time feedback through automated scanning tools, he said. The automation applies risk management requirements during the compile process, identifying vulnerabilities earlier than traditional methods.

"An engineer puts secrets in his code, and he tries to run the compile process, and we flag it with our scanning tool, and we push it back to him with a report that says, 'hey, don't put secrets in your code,'" Raley said of the quicker ATO process. "It's all of the underlying infrastructure, the security control inheritance, the deeper look from a cybersecurity perspective and the way that you can position engineers to build and deploy code securely in minutes."

Raley added that the impact needs to be much broader than a single program like Operation StormBreaker.

"We need 200 StormBreakers for the Department of War," he said. "Can we move to the concept where this is provided as a service, so it doesn't have to be redone every time?"

Photo Credit: Max Acronym/Shutterstock

“We endeavor to abstract away almost all of the underlying infrastructure complexity from the engineer and focus them only on the application layer.”

—Dave Raley, Chief Digital Business Officer, Marine Corps Community Services

GovCIO MEDIA & RESEARCH

DeepDives

Automating Software Development

Generative AI is transforming software development by automating coding, testing and documentation tasks. Organizations are using AI tools to speed development cycles, boost productivity and streamline workflows while balancing governance, security and oversight needs.

Potential Benefits

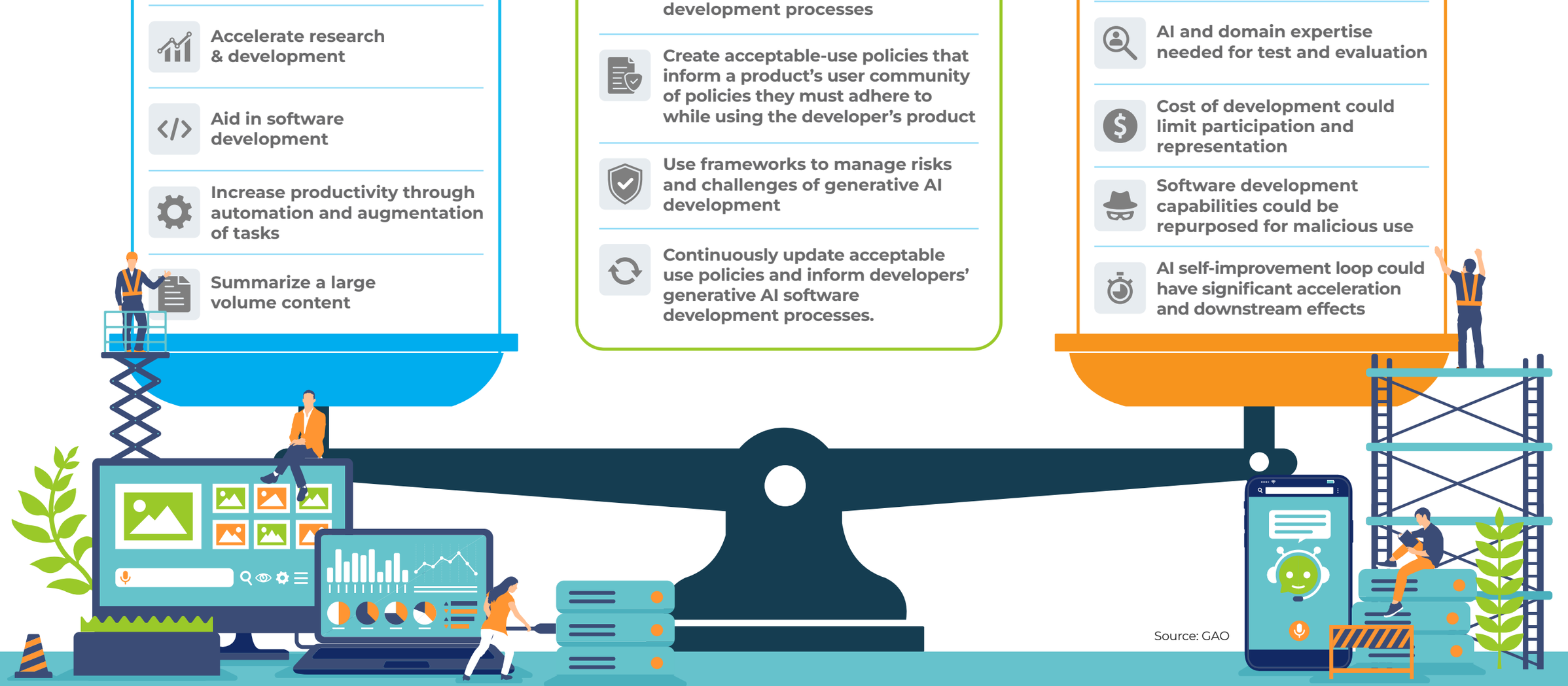
- Encourage innovation
- Accelerate research & development
- Aid in software development
- Increase productivity through automation and augmentation of tasks
- Summarize a large volume content

Potential Solutions

- Encourage the use of available NIST and GAO AI frameworks to inform generative AI use and software development processes
- Create acceptable-use policies that inform a product's user community of policies they must adhere to while using the developer's product
- Use frameworks to manage risks and challenges of generative AI development
- Continuously update acceptable use policies and inform developers' generative AI software development processes.

Potential Challenges

- Lack of understanding of generative AI could inhibit effective use
- AI and domain expertise needed for test and evaluation
- Cost of development could limit participation and representation
- Software development capabilities could be repurposed for malicious use
- AI self-improvement loop could have significant acceleration and downstream effects



Source: GAO

PARTNER INTERVIEW

GovCIO MEDIA & RESEARCH

CDW

Platform Engineering Emerges as 'Final Boss' of DevSecOps

Federal agencies are working to close gaps in automation, observability and workforce skills as platform engineering reshapes DevSecOps strategies.

What are the challenges you see government facing in platform engineering for DevSecOps?

Bockowski Government agencies often struggle with the "how to" of platform engineering and, as a result, face significant challenges in transitioning from manual ticketing to automated self-provisioning. They want to do it, but they may not understand how to put all the fundamental building blocks together.

Stimbert Some of our customers may have an entire team of people that are coding and using it regularly, but they don't have observability. They're missing part of the entire workflow that would enable them to see the end-to-end workflow and understand what's

missing. The gaps could include attracting and retaining workers with the needed skills, training, hypervisor selection or the funding to move forward. Platform engineering acts as the "final boss of DevSecOps" because it forces an agency to solve all these disparate gaps — skills, funding and technical silos — into one unified, declarative environment.

What are some successes or use cases for this technology that you've seen helping?

Bockowski I've seen successes when an agency already has an application shop. They were already doing software development and then bringing in more automation toolsets like GitLab or Terraform. They've been able to get to about 75% of a fully mature solution. They have the pipelines. The have the automated processes. Now they are trying to extend it for a complete system. After that, they will make the marketplace or app store for self-provisioning. Then the soldier will submit something or go to a site if they have access and download the solution they need.

What are you looking forward to seeing in government's use of platform engineering in the coming year?

Bockowski I'm looking forward to seeing the impact and advancement of technology with the Army portfolio acquisition executive (PAE) restructure. The goal is to shift from managing individual programs to managing holistic capabilities to deliver technology to our warfighters faster.

As a partner to the government, we're developing a platform by which you'll be able to get advanced capabilities to your systems, whether they're in the cloud or on the edge. This is critical for the government because we're going to see new challenges and new compliance issues emerging, such as preparing for the quantum environment.

Stimbert The growth as they realign these mission functions to an

> **"Platform engineering acts as the 'final boss of DevSecOps' because it forces an agency to solve all these disparate gaps — skills, funding and technical silos — into one unified, declarative environment."**
>
> **—Ron Stimbert, Industry Strategist, CDW**

organization that has responsibility for deploying platforms for the Navy.

This takes 10 or 15 different capabilities and aligns them under one organization. It's going to be very productive for those who design, build and deploy platform

We're getting to the place where an environment only exists because it's a declarative environment. It can be torn down or recreated because in that declarative environment, making changes to your configuration items becomes very easy. If you need to make a change from one type of algorithm to a quantum-resistant algorithm with infrastructure as declarative code, it becomes easier to flip that switch.

Photo Credit: ultramansk/Shutterstock

Secure Supply Chain

1000+ OEMs

Recognized Leader

CMMI Appraised

Trusted Partner

CDW Government

Compliant Solutions

CMMC Compliant

Unmatched Expertise

IT Modernization

Cyber Security

Managed IT Services

AI Strategy

Solutions Provider

Cloud Migration / Adoption

Software

IT Hardware

Staff Augmentation

Zero Trust

Oasis+

Vehicles

GSA MAS

NASA SEWP

Shield

For more information, reach out to your dedicated account team.
800.800.4239 | CDWG.com/federal

CDW®

DOW Expands DevSecOps to Accelerate Software Deployment

The Pentagon is using continuous authorization and better processes to integrate security and speed across all programs.

BY ROSS GIANFORTUNE

The War Department is using successful DevSecOps pilot programs to drive broader adoption of agile software development practices across the Pentagon, said DOW Cloud and Software Modernization Director George Lamb.

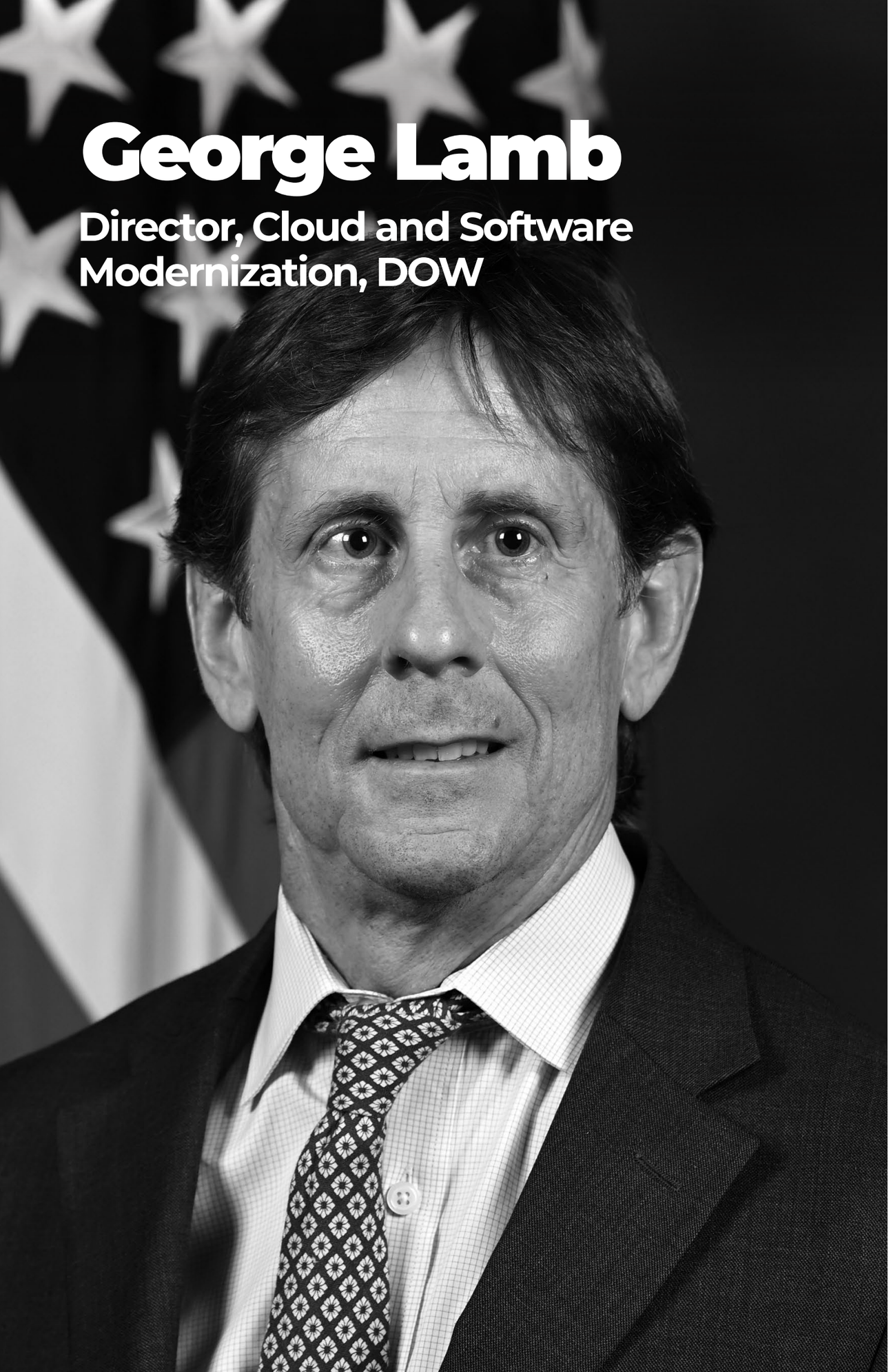
DOW is expanding the use of continuous authorization to operate (cATO) processes, automation and other modern software development approaches to accelerate deployment timelines and improve operational scalability.

"[DevSecOps] success at the CIO level [means] … more programs that are modernizing and getting into production," Lamb said. "The forcing function [is] that we're hoping to get some of these larger programs into a modern software construct."

Lamb said DevSecOps is not simply a technical framework, but a core enabler of mission success. He pointed to DOW initiatives like Platform One and Netcom as proof that DevSecOps can dramatically increase deployment speed, with some patches reaching production in as little as an hour.

"We talk about Netcom, we talk about Platform One, they are amazing technical success stories," Lamb said. (ctd.)

Photo Credit: Carahsoft



The DevSecOps Infinity Loop

Lamb said that the DOW's State of DevSecOps publication released in March 2025 proves "the technology works."

He highlighted the report's DevSecOps Infinity Loop, a figure-eight model illustrating the continuous cycle between development and operations. While the development side of the loop often receives the most attention, Lamb said the operations side is where DOW frequently struggles.

"The 'Ops' part is where we fail," Lamb said. "You think about software. The key is taking something that exists, is a software, a constructible thing, and then pushing into operations, and then getting feedback, and then feeding it back [within the DevSecOps Infinity Loop]. And that's the part that people mostly miss. How do you get it into production?"

Lamb said the feedback mechanism is central to the Infinity Loop concept. Production, he added, should be viewed as the beginning of an ongoing cycle of iteration and improvement rather than the end state.

"That feedback loop, that's really the heart of DevSecOps," said Lamb. "It's that feedback loop, the breaking down silos and wrapping the process around a repeatable loop. And then you get the cycle times: That's where the scaling is, and that's where we're hitting the problem."

Breaking down silos and embedding repeatable feedback loops, he added, is critical to achieving the speed and scalability DOW wants from modern software development.

Accelerating Authorization Through cATO

The Pentagon is working toward cATO within DevSecOps to shorten development cycles, Lamb added.

According to DOW, cATO is a significant shift in DOW cybersecurity practices that incorporates real-time assessment, zero trust principles and DevSecOps to secure the nation's supply chain against emerging threats and

improve overall cybersecurity posture.

Lamb said that cATO is not about eliminating the DOW's risk management framework but rather about transforming its application to remove impediments and accelerate processes.

"ATO is where you start, cATO doesn't stop," said Lamb.

He emphasized the importance of dashboards to provide real-time visibility into anomalies, allowing for rapid remediation of security issues. Last year, the Army nominated three software factories for cATO approval, a process that was "struggling" for two years. Lamb said pushing down authority to the services will enable broader scaling.

Commercial Software in the DevSecOps Process

Lamb stressed that DevSecOps modernization extends beyond internally developed software. Commercial off-the-shelf (COTS) software also requires automation, continuous monitoring and lifecycle management as patches and configuration changes are introduced.

The Software Fast Track (SWFT) process gets COTS software into the DevSecOps pipeline and operational more quickly, he added.

"Commercial technology is just software," Lamb said. "How do we get that commercial software into our pipeline? SWFT is a process for going to look at the authorization process."

Iron Bank, the container repository for Platform One, serves as a prime example of this process. With over 1,500 mostly commercial containers, Iron Bank scans and evaluates software and provides a risk assessment rather than a simple pass/fail. This methodology improves risk management and brings secure commercial software into the infinity loop faster.

"We put insecure software in production all the time," Lamb said, "Iron Bank scans it … We don't stop it. We just put caveats around it. We check it. We're very careful about where it's used. That's how the scaling works and

Photo Credit: PeopleImages/Shutterstock

that's where the security needs to come from."

The Evolving Landscape of Software Development

Lamb said DOW's software factory concept is continuing to evolve. Initially, there was a widespread desire to establish software factories within the military services, followed by a period of retraction due to congressional scrutiny.

"There was a time when everyone wanted to be a software factory, and then there was a time where nobody wanted to because Congress is saying we have too many software factories," Lamb said. "The new term is a software development activity."

The term, Lamb said, is part of a foundational concept driving modernization efforts. He said that the activities are more about managing full lifecycles — including configuration, cloud integration and patching.

"Software is everything," Lamb said. "Business systems, logistics platforms,

"Software is everything. Business systems, logistics platforms, even routers — everything now requires secure configuration and ongoing management."

—George Lamb, Director, Cloud and Software Modernization, DOW

even routers — everything now requires secure configuration and ongoing management."

Codified Policy and Cultural Shift

Lamb underscored the need for codified DOW instructions to mandate and further scale DevSecOps practices across the department. While guides and reference designs exist, formal instruction is the "forcing function" that will compel legacy programs, he added.

Some DOW offices are still using older development methods and need to transition to modern software constructs, agile processes and integrated testing, Lamb said. Shifting culture and making codified DevSecOps processes may be part of the implementation of DOW guidance.

"There's no instruction that says, 'Thou shalt use DevSecOps.' The closest thing that's happened recently is in the acquisition space, with the software acquisition pathway," Lamb said. "They need to start transitioning, by fiat, by directive from the department, into using an infinity loop, using agile processes, using testing that's more integrated.

Photo Credit:DC Studio/Shutterstock