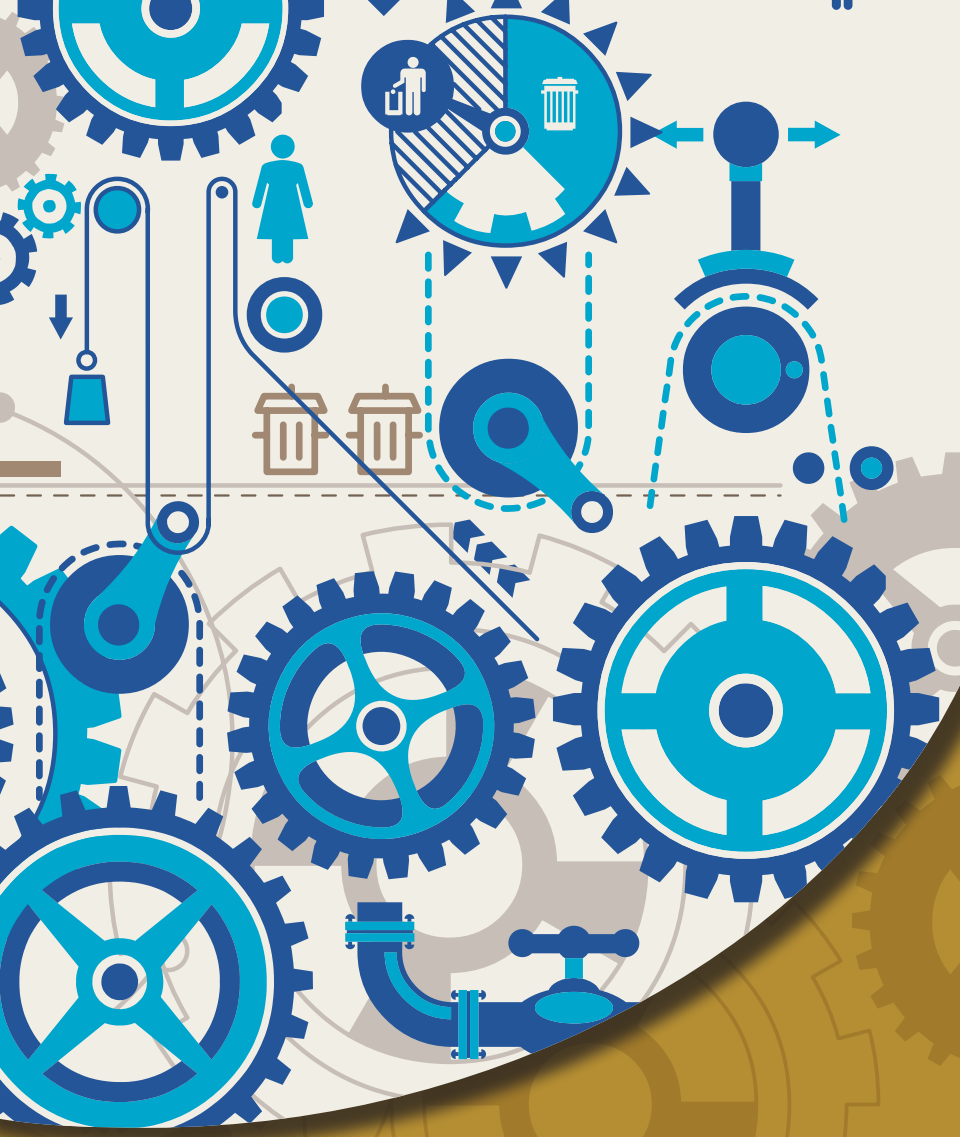


Achieving Mission Outcomes Through DevSecOps

Margie Graves
Visiting Fellow
IBM Center for
The Business of Government

IBM Center for
The Business
of Government
2021

TABLE OF CONTENTS

What is DevSecOps 4

Advantages of DevSecOps 5

Legislation, Policy, and Governance Barriers 5

Finance and Acquisition Barriers 8

Cultural Barriers to Creating Trust and Putting CX first 9

About the author 10

Contact Information: 10

For More Information 11

On behalf of the IBM Center for the Business of Government, we are pleased to present this special report on *Achieving Mission Outcomes Through DevSecOps.* The report draws on expert insights from a roundtable discussion with operational experts from DOD and industry, and reflects perspectives shared in a series of blog posts referenced on p. 11. The report addresses the critical role that DevSecOps plays to support the DoD mission.

WHAT IS DEVSECOPS

DevSecOps—short for development, security, and operations—is an approach to IT security based on the principles of the scientific method of experimentation: observe, question, hypothesize, predict, test, and iterate. This solid foundational methodology has served the STEM (science, technology, engineering, and math, including computer science) community well, and has resulted in some of the most impactful innovations and scientific breakthroughs of our time.

There is no more current or relevant proof point of the success of this approach than the rapid development of multiple COVID-19 vaccines to address and battle the pandemic. What works in medical science also works in creating emerging technologies, specifically the development of new software to support the Department of Defense (DoD) mission and, indeed, the missions of agencies across the federal government.

When using DevSecOps, the organization creates a pre-approved software development environment, inclusive of security elements. Developers in this environment can experiment, code, test, prove, or disprove initial hypotheses about how the code will work for the user; adjust the software build according to what they learn; and then continue iterating. Security is an integrated part of the development build, incorporated into all stages of the software development workflow, and "owned" by the entire DevSecOps team. Capabilities and features are continuously developed and integrated through this agile process until the full mission intent is met.

ADVANTAGES OF DEVSECOPS

Characteristics of a DevSecOps environment include standard approved tools that allow for the creation of modular open systems architectures with application programming interfaces (APIs). Open modular architectures let developers use building blocks to more rapidly incorporate changes in feature sets in response to evolving mission circumstances, unplanned or unanticipated requirements, or the changing context of mission execution. These tools not only work for greenfield development but also can work in brownfield upgrades where legacy systems are abstracted from the workflow, affording developers the opportunity to make disparate systems, old and new, interoperable.

This flexible environment also continuously integrates end-to-end workflows and feature sets, and has security built in as a continuous integration element. The development pipeline steps are scripted and automated so that each iteration of the software or "sprint" can be delivered more rapidly simply by executing the script. In summary, using the DevSecOps approach assists developers in delivering mission capability to the frontlines in a more effective and efficient manner, lessoning the "time to market" while continuously incorporating security as part of the product.

The advantages of the DevSecOps approach are well known and documented in both the private and public sectors. However, the adoption rate in the public sector lags. The next sections explore explanations for this lag, and identify actions across the development community that can mitigate barriers and ultimately accelerate adoption of DevSecOps.

LEGISLATION, POLICY, AND GOVERNANCE BARRIERS

Grace Hopper, the iconic computer scientist and United States Navy rear admiral, once said,

> The most damaging phrase in the language is 'We've always done it this way.'

Legislation, policy, and governance processes are generally codified to address certain circumstances at a point in time. But policy and governance approaches inevitably age out of relevance and must also be refreshed. Governance ensures that programs and projects have the best chance of success by rigorously applying review processes and rule sets. It is human nature to become comfortable and complacent with governance parameters and to miss the inflection point where the process or rule sets either no longer work at all, or do not work for specified circumstances. When legislation, policy, or governance becomes a blocker to the solutions, methodologies, and mission improvements that agencies must implement, this becomes the inflection point where governance must also change.

In the federal government—and particularly with the planning, programming, budgeting and execution (PPBE) and program objective memorandum (POM) processes at DoD—existing policies and governance were originally built to support the development and deployment of physical assets: planes, ships, and tanks. The lifecycle for such assets is not just multiyear but multi-decade. Planning for such delivery programs loads all of the planning elements—such as the setting of requirements, risk analysis, milestone identification, delivery timeline, and acceptance criteria—at the very beginning of the program lifecycle. The design parameters of the assets are generally known through a long history of delivery of similar assets, and variability rarely occurs or occurs on an elongated timeframe.

This governance approach does not match today's development and delivery needs for emerging technologies and software. The waterfall approach to software development is an artifact of this historical governance process. Under the waterfall approach, functional requirements and technical approaches were planned and approved at the outset of a program, sometimes as much as three years in advance of funding. By the time a program was truly initiated, it was likely that the risk profile had changed, the requirements were obsolete, and the solutions were "yesterday's technology deployed today."

Also, in the waterfall method, the warfighter or the customer was never effectively embedded in the process of development; feedback loops only occurred at specific milestone points. The milestone points were few and far between and did not provide feedback in a timely enough fashion to adjust course without significant rework, accompanied by schedule and cost overruns. Software products could not be "accepted" until all of the features and requirements in the obsolete requirements documents had been delivered. Many of these requirements were features that would never even be used by the warfighter.

In the military environment of today, where the next battlefield frontier is cyber warfare, the threats are constantly evolving and the technology refreshes on a short cycle. Solutions change and new technologies emerge rapidly. Every scenario and the accompanying technology solution cannot be forecasted with any certainty upfront.

The DevSecOps methodology provides a proven, modernized approach to software development that addresses many of the governance flaws mentioned previously. However, legislation, policy, and governance have not changed enough to accelerate the adoption and effective execution of DevSecOps. Valiant efforts have been made and continue, as evidenced by updates to Office of Management and Budget (OMB) policies such as Cloud First and Trusted Internet Connection (TIC) 3.0, and updates to the National Institute of Standards and Technology (NIST) Risk Management Framework and the NIST 800 series. But the path could be smoother, with much more work required to clear obstacles. So where can efforts be focused and how might the methodologies for creating policy and executing governance be changed?

Flexible legislation and policy should support a directionally correct intent, without prescribing a detailed approach. Legislation and policy should reflect the “commander’s intent.” Details can be fleshed out in guidance, best practices, and playbooks—all of which do not require a protracted process of going through another cycle of legislation and policy to evolve and change.

Measurement and audit of the success of new methodologies such as DevSecOps should draw on new metrics, not historical approaches. For example, measure the velocity of user story delivery cycles, customer satisfaction (CX), and reduction of technical debt. Also be willing to change the traditional definition of a dollar-based return on investment (ROI) to incorporate measures other than cost reduction. Measurements must reflect ROM, return on mission—which reflects greater mission impact achieved.

The federal government has the power to convene operational experts and to work with standards and governance bodies to ensure alignment and directional consistency. OMB, NIST and auditors in the U.S. Government Accountability Office (GAO) and Office of Inspector General (IGs)—specifically, those who measure program success—can enable rather than constrain effective implementation of DevSecOps. When the voice of the mission operators is heard, policies from OMB, NIST Federal Information Processing Standards (FIPS) and DoD Security Technical Implementation Guides (STIGs) will more closely reflect the perspective of the operating entities. Mission operators must be a part of the solution and serve as a proof point for the new policy and governance framework.

Agencies can question the status quo and challenge the perception that the production of multitudes of documents and reams of forms and paper reflect a well-run or well-planned program. Demonstrable delivery of user features in shorter cycles, coupled with high customer experience scores, better reflect success and should provide some of the measurements incorporated into the governance processes.

FINANCE AND ACQUISITION BARRIERS

Alongside a rethinking of policy and governance approaches sits a rethinking of business models, including the adoption of flexible funding models and innovative acquisition approaches.

Continuous innovation and transformation require secured flows of funding in order for developers to effectively address technical debt (e.g., the cost of modernizing legacy systems). There are many funding mechanisms available such as the Technology Modernization Fund, agency working capital funds, base budgets for programs, and operation and maintenance (O&M) funds. Developing the right mix within the funding strategy will enable sustainability. No single tactical edge investment can solve every problem or carry the burden of funding. Support across the enterprise can involve portfolio management to organize, track, and address the larger, common issues. Leaders can then pull from multiple sources of funds to address common issues for the good of the whole organization.

Similarly, acquisition approaches can complement the way that technology is delivered. Contracting can be more effective using level of effort (LOE) or time and materials (T&M) approaches, and by avoiding prescriptive requirements through use of a statement of objectives (SOO) rather than a statement of work (SOW). Whenever possible, we should take advantage of no-code, low-code platforms and software as a service. Metrics based on outcomes are key. A solution is only relevant to the extent that it provides measurable impact and improvement in support of the warfighter.

CULTURAL BARRIERS TO CREATING TRUST AND PUTTING CX FIRST

Government entities often operate in a manner driven by organizational construct rather than horizontal workflow delivery. This creates a number of issues for DevSecOps. Fostering an environment of trust among all participants in the DevSecOps cycle requires eliminating stovepipes and forming integrated multidisciplinary teams. The makeup of these teams includes program leaders, customers, developers, and finance and acquisition specialists. The team should also include members who support the legacy infrastructure as well as those creating new code. Both are required for a successful deployment.

Effective and continuous communication between users and developers promotes an exceptional customer experience. Developers can benefit from observation of frontline operations. The principles of human-centered design apply. Users must contribute to developing hypotheses developed regarding the importance of any software feature. Frequency of use for specific features should be monitored so that developers can target what works well and why, and what to discard. Developers must support shedding features. The risk of recognizing failure has higher consequences for the public sector than for the commercial tech sector, given government cultural norms that tend toward risk aversion. Only through helping government understand and reflect risk can the full advantage of experimentation and innovation be realized.

Government can work with industry partners and have more open conversations about solutions that vendors provide to their customers. In addition, building relationships with commercial enterprises that have similar profiles—and discussing how they resolved common issues within their own operations—encourages a learning process that benefits all parties.

Building this circle of trust will enable successful application of DevSecOps to achieve successful outcomes in improving customer experience and supporting defense outcomes.

ABOUT THE AUTHOR

MARGIE GRAVES

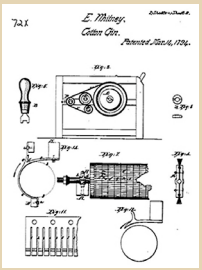
Margie Graves is a Visiting Fellow with the IBM Center for The Business of Government. She is the former Deputy Federal CIO for the Office of Management and Budget. She led the Office of the Federal Chief Information Officer efforts to drive value in Federal IT, deliver digital services, protect Federal IT assets and information, and develop the next generation IT workforce. In her previous role, Margie worked to improve the way Government delivers results and technology services to the public. She drove elements of the President's Management Agenda; IT Modernization, Data as a Strategic Asset and Workforce of the 21st Century. Margie also served as the Deputy CIO at the U.S. Department of Homeland Security (DHS). As the Deputy CIO, she had oversight of an IT portfolio of $5.4 billion in programs. She managed the operations of the Office of the Chief Information Officer, covering the functional areas of Applied Technology, Enterprise Architecture, Data Management, IT Security, Infrastructure Operations, IT Accessibility, Budget and Acquisition.

CONTACT INFORMATION:

Email: Margaret.Graves@ibm.com

FOR MORE INFORMATION

To learn more on this topic, reference a series of three blogs created for the IBM Center for the Business of Government:

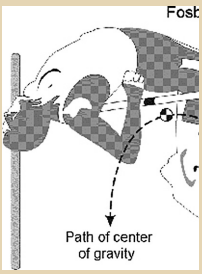


Achieving Substantial Gains in IT Performance Across Government Through DevSecOps

by Chris Yates
Senior Solutions Architect
Red Hat

What does celestial navigation have to do with DevSecOps, artificial intelligence, and machine learning?

by Chris Yates
Senior Solutions Architect
Red Hat



Promoting an Innovative Workforce Through DevSecOps

by Matt Gordon
Managing Consultant
IBM Global Business Services

About the IBM Center for The Business of Government

Through research stipends and events, the IBM Center for The Business of Government stimulates research and facilitates discussion of new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

About IBM Global Business Services

With consultants and professional staff in more than 160 countries globally, IBM Global Business Services is the world's largest consulting services organization. IBM Global Business Services provides clients with business process and industry expertise, a deep understanding of technology solutions that address specific industry issues, and the ability to design, build, and run those solutions in a way that delivers bottom-line value. To learn more visit ibm.com.

For more information:
Daniel J. Chenok
Executive Director
IBM Center for The Business of Government

600 14th Street NW
Second Floor
Washington, DC 20005
202-551-9342

website: www.businessofgovernment.org
e-mail: businessofgovernment@us.ibm.com

IBM Center for
The Business
of Government

Stay connected with the IBM Center on:

or, send us your name and e-mail to receive our newsletters.