Market Connections™
Research you can act on.

maximus

TAPPING DEVSECOPS TAKES FEDERAL MODERNIZATION TO THE NEXT LEVEL

INTRODUCTION

The federal government is focused on achieving technology resiliency that balances workforce, cost, cybersecurity, and mission enablement — addressing barriers to modernization at every turn. To better understand how agencies are reaching their modernization goals, Maximus partnered with Market Connections to include a series of questions about application modernization priorities and challenges in the November Federal IT Omnibus poll, a monthly poll of federal IT decision makers[1].

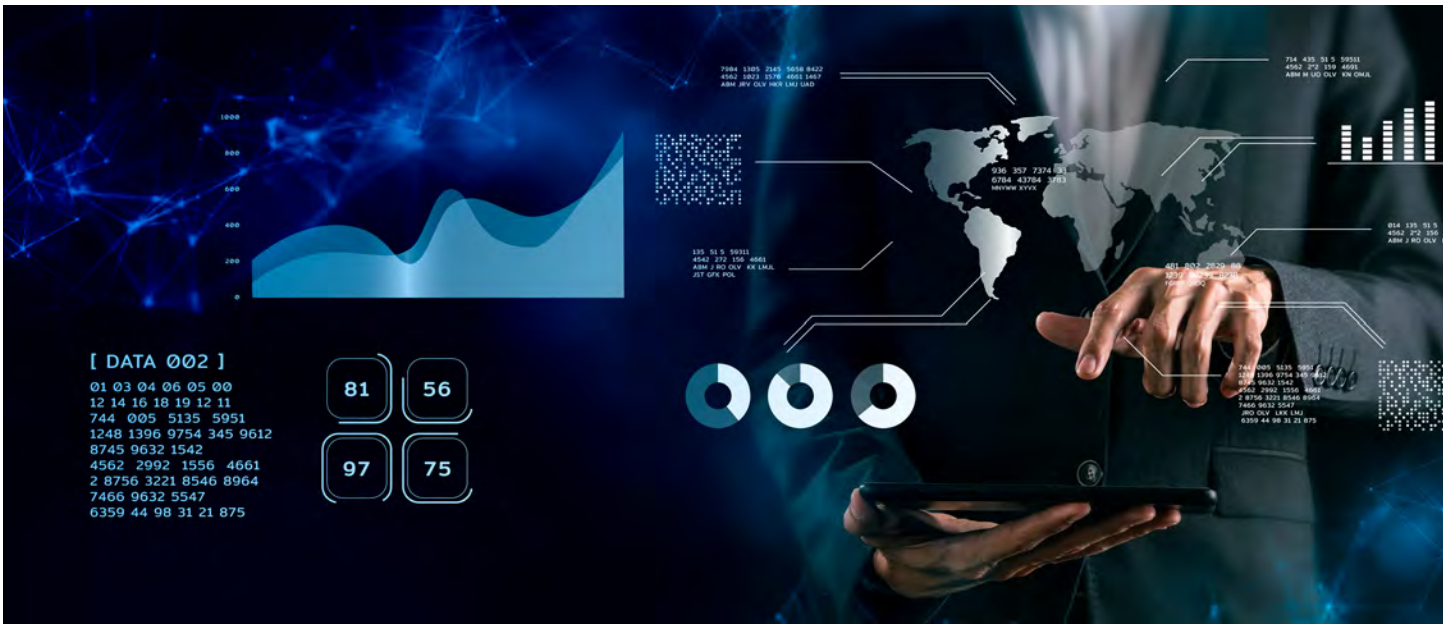
ABOUT THE STUDY

The Market Connections monthly Federal IT Omnibus Survey is a poll of government leaders designed to provide a point-in-time look at primary public sector sentiments across federal technology areas. In November 2022 the poll included seven questions regarding application modernization. Of the 168 respondents, 63% work for a Federal Civilian agency and 37% are with Defense/Intelligence agencies. Almost all (96%) have a roll in the contractor selection process, and all manage contractors on some level. One-third of respondents have an IT/MIS/IRM role within their organization.

[1]The Market Connections Federal IT Omnibus Survey is a monthly poll of government leaders designed to provide a point-in-time look at primary public sector sentiments across Federal technology areas. Specific details about the November poll are located on the About page of this document.

[2]Lamar Johnson. "FITARA 12.0: 60 Percent of Fed IT Spending Maintains Legacy Systems." Meritalk. July 21, 2021.

[3]Ibid.



Legacy systems significantly impact agency mission enablement.

60% *of the federal IT technology budget is spent on maintaining legacy systems[2].*

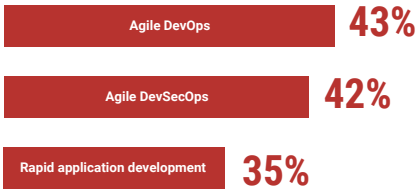
40% *of federal IT managers say staff recruitment is their biggest concern as the aging federal workforce retires[3].*

Legacy systems are **more vulnerable to cyberattacks.**

Without vendor support, **legacy systems create functional barriers** *to implementing IT projects.*

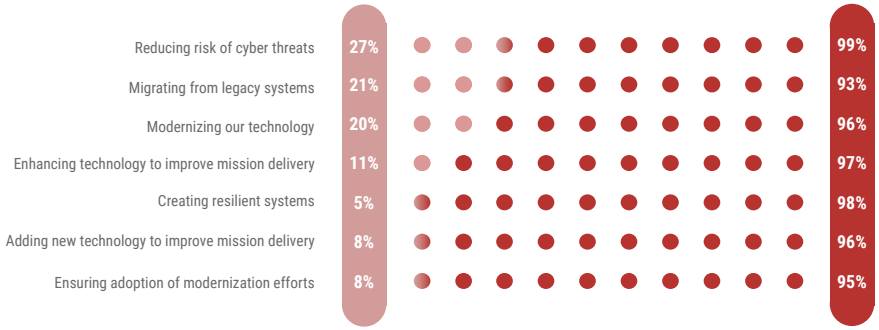
Current development practices can help meet priorities
DevSecOps usage has increased for about 60% of Feds.

Top 3 development practices



Most respondents use 2-3 practices—
Agile practices are the most common.

A DevSecOps approach facilitates meeting agency priorities.
Migrating from legacy systems, modernizing technology, and enhancing technology all support the 2024 priority of creating resilient systems.

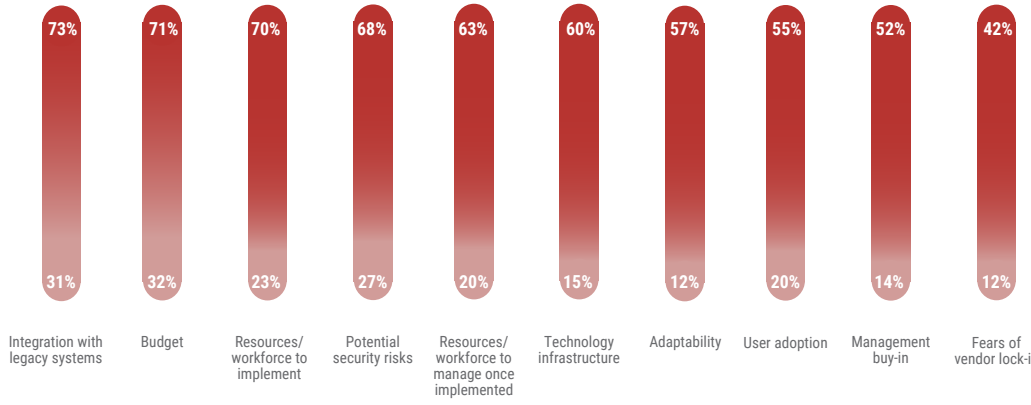


Q. What is your agency's biggest technology priority in the next 12-24 months?

Q. What are your agency's technology priorities through 2024? Very big priority

Biggest priority in 12 to 24 months
A priority by 2024

Integration with legacy systems slows modernization efforts.
Three quarters say challenges around legacy system upgrades are a barrier to modernization. Nearly one-third say it is a large barrier. While budget and staffing are barriers, security risks represent the third largest challenge.

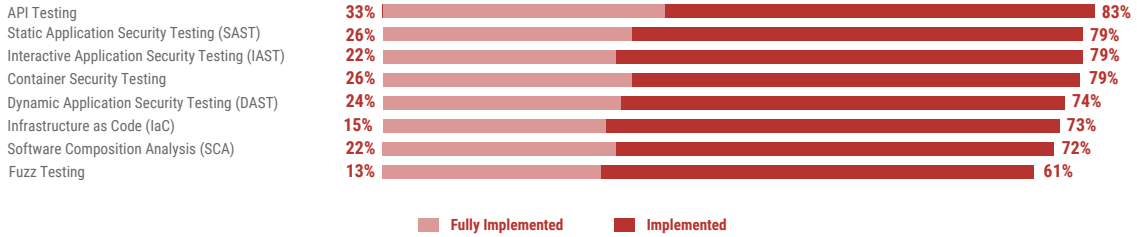


Q: How much of a barrier are each of the following to your agency's modernization efforts? Yet only 21% of Federal IT managers say migrating from legacy systems is a big priority in the next 12 to 24 months.

Q. What are your agency's technology priorities through 2024? Very big priority

A LARGE barrier
A barrier

Most testing methods are only partially implemented into agency continuous integration pipelines.
Continuous integration pipelines sit adjacent to DevSecOps in terms of processes aimed at improving the quality and services of software applications. CI ultimately pipelines enable developers to continuously test and validate code security.



MAXIMUS' PERSPECTIVE

A COMPREHENSIVE APPROACH TO FEDERAL DEVSECOPS

As agencies move away from legacy systems, moving to modernizing that make it more effective and efficient to meet the mission, DevSecOps has emerged as a critical approach to help the federal government transform while overcoming rising challenges around security and compliance. By tapping into a DevSecOps approach, agencies can automate their security processes, detect and remediate vulnerabilities early in the development cycle, and improve the overall quality and reliability of applications.

Indeed, agencies across the federal landscape are tapping into the approach, with DevSecOps usage rising 60% for federal application development teams. The reason behind the increase in popularity is simple, it offers major advantages over traditional software development methods. Historically, software development and security were seen as separate processes, with security only addressed after the development process was complete. This was problematic for a key reason: It wasted time and resources.

With DevSecOps, security is integrated into the development process from the start, making development faster and more secure. It actually saves time instead of wasting it — and because security is considered from the start instead of tacked on at the end of a development process, it places systems and applications in a more defensive position from the outset.

But not all DevSecOps approaches are created equal. It's vital to ensure that as teams tap into a DevSecOps approach they use a structured process that facilitates and encourages collaboration between development, security and operations team. Maximus' approach does just this. We focus on implementing security controls throughout the software development lifecycle, starting from the design phase and continuing through development, testing and deployment. Our arsenal of automation tools and processes helps accelerate the delivery of secure and compliant applications.

MYTH 01

Modernizing for the Present and Future

Legacy systems continue to create a drag on modernization efforts, with 73% of federal IT leaders saying legacy systems are a barrier to modernization, not to mention the fact that legacy systems aren't equipped with the computing power necessary to run and install modern day security patches, thus making them more susceptible to cyberthreats. In fact, according to recent research from the Government Business Council, reducing the risk of cyberthreats is the primary driver of current and future technology priorities.

DevSecOps, can help agencies implement and initialize modernization processes. To this effect, with the aim to help agencies modernize legacy systems effectively, sidestep vulnerabilities, and leapfrog into the future, we have developed a range of capabilities, including cloud migration, application modernization, data analytics, cybersecurity and digital transformation. These capabilities can help agencies improve their operational efficiency, save money, increase security and ultimately provide better services to the public.

But we don't stop there. We understand that not all agencies are created equal and that a successful modernization effort requires a holistic approach that takes into account current challenges as well as future needs. To address all these variables, we collaborate closely with our customers, including the Army Materiel Command, Department of Homeland Security, and the Internal Revenue Service among others, to understand their specific mission objectives and business requirements, like providing quality educational guidelines or distributing necessary materials across the U.S. supply chain, and deliver secure, innovative applications to meet those needs.

These solutions are designed to be scalable, flexible and resilient. We incorporate the latest technologies and best practices to ensure our government customers meet their mission objectives, whether it's getting applications into the field faster by using low-code/no-code platforms or tapping into user-centered design approaches to deliver more intuitive, streamlined services to constituents.

Our approach involves a significant amount of standardization in our pipeline, including continuous integration capabilities that enable developers to continuously test and validate the security of their code as it is being developed. This standardization makes

it easy to templatize each layer and ultimately allows developers to identify and fix security issues early on, before they can be exploited by attackers. What also sets us apart is our code-shipping capability, which includes automation tools that generate a standardized pipeline and streamline the code-shipping process for developers. This pipeline provides an integrated framework and end-to-end security to drive process flow and provides defense-in-depth within the production environment. That allows us to deploy in a multi-cloud environment and on-premises if our customer doesn't already have that capability.

MYTH 02

Busting Common DevSecOps Myths

Despite the numerous advantages DevSecOps offers and the growing interest among agencies development teams, some agencies remain hesitant to adopt this approach. A well-designed process can help agencies overcome hesitancies that are based on outdated understandings of DevSecOps and fully understand and embrace the process.

One common misconception is that DevSecOps is too difficult or expensive to implement. However, with the right approach, it can be adopted efficiently and cost-effectively. The key is to use a trusted partner with experience in implementing DevSecOps best practices. Such a partner can guide the agency through the process, provide expert framework and help overcome potential challenges.

Additionally, breaking down the implementation into smaller steps and gradually transitioning to a DevSecOps approach can also make it more manageable.

Another myth is that DevSecOps is only for large organizations with vast resources. The truth is, even small organizations can benefit from improved collaboration, faster time-to-market for applications and increased security with greater compliance. Maximus' structured process can help any organization overcome these concerns and reap the benefits of DevSecOps.

Finally, a popular misbelief is that DevSecOps is only relevant for development teams. However, DevSecOps involves everyone who works with an application or system, including security assessors, compliance teams, procurement, developers, engineers and database managers. It requires a cultural shift where everyone embraces DevSecOps practices.

We provide agencies with a comprehensive and tailored approach to DevSecOps, including training and support to overcome cultural barriers. Our use of automation and other tools makes the process more efficient and cost-effective. We also ensure agencies' DevSecOps processes comply with relevant regulations and standards.

MYTH 03

How to Get Started

New research shows DevSecOps continues to gain steady traction in the federal government. In a Federal IT Omnibus Survey conducted by Government Business Council, over 70% of respondents said their agency has fully embraced DevSecOps modernization. Forty-two percent say their agency uses Agile DevSecOps.

However, for IT leaders whose agencies have yet to fully embrace DevSecOps, getting started can seem overwhelming.

Our recommendation is to start small and focus on incremental improvements. By identifying a specific application or process that can benefit from DevSecOps, agencies can gain experience and build momentum. Finally, it's important to involve all stakeholders and communicate the benefits of DevSecOps in terms of improved security, compliance and operational efficiency.

Doing this helps agencies successfully adopt DevSecOps practices while sidestepping common roadblocks that can emerge during the implementation.

Remember: Embracing DevSecOps may seem intimidating at first, but it's worth the effort to make your agency more stable and secure as you build the future of government.

James Bench *is vice president of technology consulting services at Maximus and*

Frank Reyes *is a cloud solutions leader at Maximus.*

LEARN MORE