HOW THE FEDERAL GOVERNMENT WILL WIN WITH THE CLOUD

January 2023

SAIC

Table of Contents

Executive Summary

For years, the federal government has been on a cloud migration journey — one that has shifted from simply moving workloads to the cloud to harnessing the power, resiliency and agility of cloud-native services. Today's cloud environment offers incredible potential for delivering mission and business outcomes, but also creates an added layer of complexity in agency IT environments.

As this cloud complexity grows, agencies face the challenge of adopting new technology effectively and efficiently while also providing security and a good customer experience. Winning with the cloud means not only continuing to mature cloud environments but also adopting enablers such as DevSecOps (development, security and operations) and AI (artificial intelligence). From a development perspective, DevSecOps is emerging as the way to address implementation challenges. And as serving the mission and meeting customer expectations become more complex, AI is a key enabler for innovations that will drive agencies forward.

Since embarking on the cloud journey, what triumphs and obstacles have agencies met, and what is next? SAIC partnered with Market Connections to:

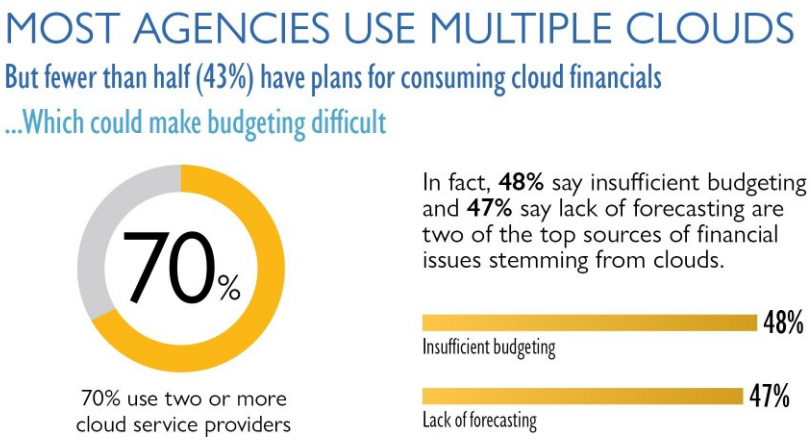
- Assess confidence levels and challenges in cloud technologies and management
- Determine the status and obstacles of implementing a DevSecOps strategy
- Understand the perceived benefits and potential barriers to implementing AI technology tools

The following report presents the findings and explores what those findings mean going forward.

Cloud Maturity Today

Agencies continue to mature when it comes to the cloud: in FY21, federal cloud spending reached a high of $10.8 billion and is increasing by an average of $1.6 billion per year — indicating cloud investment will continue to increase[1].

As spending increases, agencies are often finding they need more than one cloud to meet their needs. While nearly all federal government employees use at least one cloud, 70% use two or more. The top three are Microsoft Azure, Amazon Web Services (AWS) and Google Cloud (not surprising, given that commonly used collaboration applications Office365 and GSuite are already included in Microsoft and Google clouds, respectively).



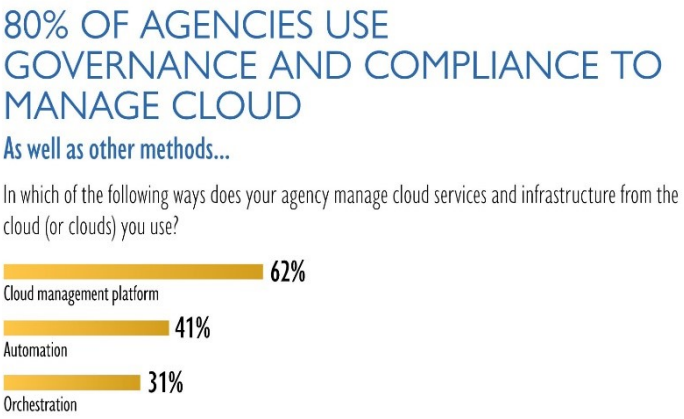
How does the government benefit from this cloud usage? Respondents believe that adopting more than one cloud allows agencies to take advantage of the best innovations from cloud providers, ensuring they have the right tool for the right job.

However, with all of the benefits comes the need to monitor spending. Insufficient budgeting, lack of forecasting and multiple bills in disparate formats are identified in the study as the leading financial issues when consuming services from multiple clouds. Nearly one in five (17%) blames incorrect billing as a financial concern. Despite this reasonably high trust that billing is not faulty, "paying the utility bill on time" with regard to cloud requires a very high level of effort due to compliance requirements.

The truth is that the more difficult it is for agencies to plan and forecast financially, the less money they have to spend on enablers like DevSecOps and AI. Having strategies for cloud financials could help with that. Regardless of the fact they're using multiple clouds, fewer than half of respondents say their agency has a plan for consuming financial information for multiple clouds. Of those who do, most are either using multiple contracts or both multiple and single contracts.

Respondents prefer multiple contracts: nearly half (45%) use many contracts, compared to one-quarter who use a single contract. Three in 10 use both single and multiple contracts for financial information.

"It is interesting to note that this data contrasts with the methods used by the intelligence community and DOD to leverage the full weight of their agencies and take maximum advantage of their buying power to drive economy of scale," said Bob Ritchie, SAIC's chief technology officer.



Uniform cloud management, especially when using more than one cloud, mitigates financial and other challenges. Respondents today are using various approaches to achieve this. Governance and compliance are by far the most popular methods (80%), followed by 62% who use cloud management platforms and 41% who use automation.

"Utilizing reusable infrastructure as code, cloud-native services, and centralized governance and cyber security operations support these top three methods as they standardize and automate the management of cloud, streamline security and compliance efforts, reduce attack surface, and accelerate speed to value," said Ritchie.

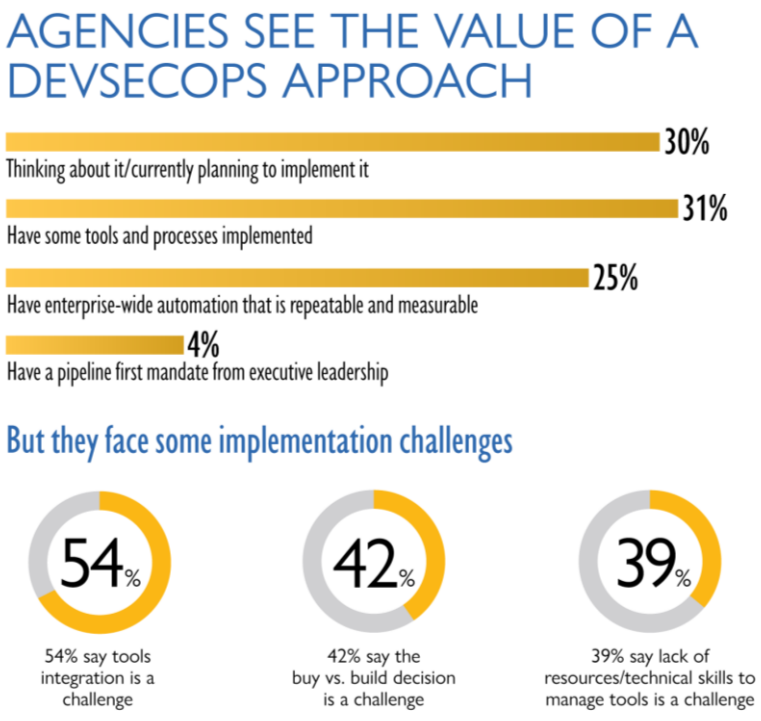
Cloud Development Now and in the Future

Nearly half of respondents say their agency handles multiple cloud deployments per day. Only one in seven reports deploying to production less than once each month. While one-third say that code change to production takes less than a week (and 12% say less than an hour), more than one-third say code change to production takes more than a month. A full 13% report that it takes less than an hour to fix outages; 83% say it takes less than a day. Just 4% say these outages take

more than a day to resolve. Only 10% report that production changes result in incidences or outages "often." However, the potential for these incidents to have catastrophic impacts due to lapsed services or cybersecurity risks remains high.

"DevSecOps minimizes the impact of code changes to production by increasing code quality, identifying and mitigating vulnerabilities early, and accelerating production recovery and problem resolution. One of the tenets of DevSecOps is that developers make small, frequent changes to production so that changes are less disruptive and easier to understand. Should a problem arise, it's much easier to track the problem and pull it out of production. Overall, a DevSecOps approach and cloud adoption provide agencies with increased agility, security, speed and quality for IT modernization initiatives," said Rana Barzegar, SAIC's senior director of Software Innovation Factory.

Agencies see the benefits of this approach: 90% of respondents are somewhere in the process of implementing DevSecOps. Three in 10 have some tools and processes implemented, and another 25% say they have enterprise-wide automation. They find the plethora of available options a challenge when implementing DevSecOps — nearly four in 10 say they struggle with having too many options. There are slight differences between DOD and civilian: 37% of DOD employees find too many options a challenge versus 32% of civilian employees.



Preferences for purchasing DevSecOps services vary. More than 40% report buying an integrated on-premise stack, but 30% prefer to build a custom tool suite. A quarter of all respondents buy software-as-a-service stacks. Integration is by far the biggest challenge for respondents when it comes to implementing DevSecOps. About 40% say the buy-versus-build decision is a challenge; civilian employees are more likely to struggle with this decision than their DOD counterparts (49% vs. 35%, respectively).

In terms of procurement, more than four in 10 are open to both buying from a commercial vendor and buying from another government agency, although only 16% say they are buying from another government agency right now.

Depending on the needs of the agency, preferences and challenges may differ. Buying a DevSecOps platform and adopting it across the enterprise allows an agency to focus on mission-critical tasks (rather than on caring for the platform). Some use cases require custom builds due to their nature. However, running your own DevSecOps platform, especially at higher classification levels, is increasingly difficult to resource as the government continues to face IT recruitment issues and cybersecurity skills gaps.

On the Horizon… AI Disruptions

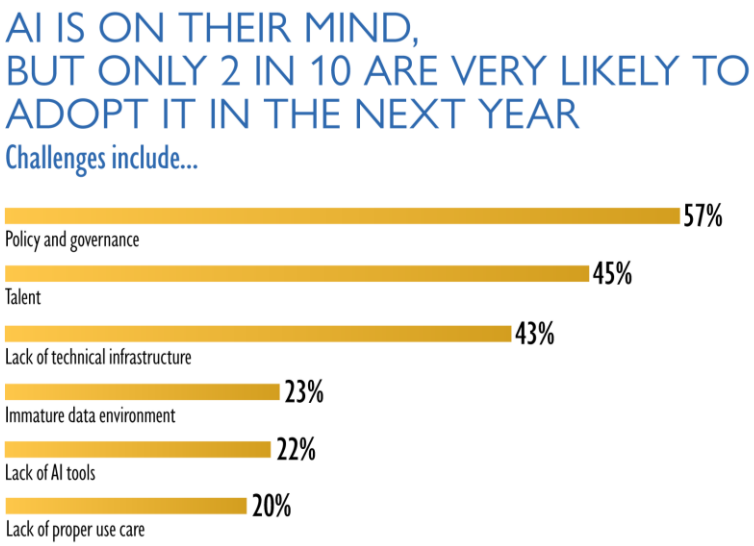
"As government moves into cloud-native development and looks to use technology to further enable the mission, AI will become critical as a key enabler for the innovation that meets the government's future needs. Its ability to automate repetitive processes with intelligence — and bring intelligence to many tasks — makes it a highly disruptive capability," said Jay Meil, SAIC's chief data scientist and director of AI.

AI is on respondents' radar, but fewer than one in five is "very" likely to adopt AI in the next year— indicating that AI adoption is not a priority at this time. Agency readiness may be the reason: one-third do not believe their agency is ready for AI, and 38% do not believe their governance and policy is mature enough to support it. Only 14% call themselves "very" ready for AI; another 12% give their readiness a "4" on a 5-point readiness scale.

The top obstacle to AI implementation (other than lack of agency readiness) is policy and governance (57%), which, given the relative nascency of AI in government usage, makes sense. For AI and machine learning (ML) to be effective, agency data needs to be clean, making data hygiene a component of policy and governance. Additionally, although there are some AI guidelines (such as the Department of Energy's AI Risk Management Playbook) at the federal level, most agencies have yet to develop their own policies. Nearly half of the respondents also cite a shortage of talent (45%) and lack of technical infrastructure (43%) as obstacles.

In addition, nearly half (47%) are concerned that AI implementation will disrupt operations. DOD personnel (54%) were more concerned about AI disruptions than civilian employees (39%).

"This data indicates a possible misunderstanding about what it takes to implement AI/ML. It is not necessary to have the perfect infrastructure, data governance or efficiency everywhere before integrating AI/ML. AI/ML in the form of data labeling or natural language processing can actually help progress data governance. Furthermore, these tools can be valuable right now in helping with manual or tedious processes to demonstrate the benefit and introduce the workforce to AI/ML in a more approachable manner. AI/ML is here to augment human intelligence rather than replace it, and by freeing the workforce to focus on analysis, agencies are able to elevate mission outcomes," said Meil.



Based On Survey Data, Here Are a Few Ways to Mitigate Risk

Today's cloud journey has expanded to involve development methods and technologies that enable mission readiness and deliver mission outcomes. Whatever stage of the cloud journey you are in, the secret to success is being able to go forward with organized and cohesive plans and tactics that provide you with a clear picture of what's occurring in your IT and cloud environment. These three steps can help you get there:

1. Explore: Assess the as-is state and develop a cloud strategy with a target architecture and security objectives. This includes a plan for migrating applications and workloads to a desired state that aligns with your cloud and mission goals.

2. Migrate: Make applications and workloads cloud-ready and move them to the cloud—whether that means a single application, multiple applications or your entire portfolio. This may include retiring inefficient applications and refactoring them for the cloud, which will lower sustainment costs and provide efficient, commercial-like user experiences.

3. Operate: Choose the cloud management services that fit your agency. Consider daily operations and maintenance activities or managed service models.

Following these three steps, along with implementing a robust DevSecOps approach and continuing to explore innovative ways that AI can work for your agency, will help:

- Take you on a faster path to compliance with government cloud security controls
- Enhance your agency's agility by allowing personnel to quickly develop and integrate innovative new applications and business services with more consistent and commercial-like user experiences
- Bring business agility and financial benefits starting from the first day and deliver even greater cost savings and organizational efficiency over time
- Make you ready for continuous performance and efficiency improvements through innovations and new and emerging technologies

In summary, these recommendations are for your consideration and use as you go on your own path to discover what it means to win with the cloud.

About the Study

Market Connections and SAIC partnered to design an online survey of 375 IT and business influencers and decision-makers across defense and civilian agencies within the federal government regarding their use of IT and digital services. The survey was fielded from Oct. 15 to Nov. 3, 2022.

About SAIC

SAIC® is a premier Fortune 500® technology integrator solving our nation's most complex modernization and readiness challenges across the defense, space, federal civilian, and intelligence markets. Our robust portfolio of offerings includes high-end solutions in systems engineering and integration; enterprise IT, including cloud services; cyber; software; advanced analytics and simulation; and training. With an intimate understanding of our customers' challenges and deep expertise in

existing and emerging technologies, we integrate the best components from our own portfolio and our partner ecosystem to rapidly deliver innovative, effective, and efficient solutions.

We are a team of 25,500 strong driven by mission, united purpose, and inspired by opportunity. Headquartered in Reston, Virginia, SAIC has annual revenues of approximately $7.1 billion. For more information, visit www.saic.com.

About Market Connections

Market Connections, a portfolio platform of GovExec, delivers actionable intelligence and insights that enable improved business performance and positioning for leading businesses, trade associations, and the public sector. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among the public sector and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education. For more information visit: www.marketconnectionsinc.com.