

SPONSORED CONTENT

**CSO**  
FROM IDG



**ACCELERATING GOVERNMENT  
INNOVATION AND  
MODERNIZATION WITH  
CLOUD**

Adopting cloud technologies can not only open the doors to agility but also improve the effectiveness of services and internal IT operations.



## **GOVERNMENT AGENCIES ARE AT AN IMPORTANT CROSSROADS.**

For years they've faced mandates to modernize IT, but many have made limited progress. Now, with increasing citizen demands and other mission requirements, agencies are under pressure to adopt newer technologies. Faced with aging systems that are not up to the task — along with the need to reduce security risks and improve efficiencies — cloud is emerging as the primary vehicle for transforming government agencies.

This IT modernization trend is essential to increasing efficiencies, flexibility, and scalability while also reducing risks. Given the limited IT resources in most government agencies, cloud services help minimize the need for maintenance and management, freeing agency personnel to focus on innovations that drive success of mission objectives.

In the past, ensuring effective risk management has been a primary gating factor in government adoption of cloud. But now, U.S. Federal Risk and Authorization Management Program (FedRAMP) authorized secure cloud-based services are available to help accelerate modernization efforts. (FedRAMP provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud products and services.)

Cloud services have also proven to help reduce security risks, improve efficiencies, drive initiatives to meet agency goals, deliver improved customer experiences, and achieve other mission objectives.

## **The Modernization Imperative**

Government agencies are facing a new level of urgency to modernize. In May 2017 President Trump issued an executive order tasking various agency heads to focus on strengthening the cybersecurity of federal networks and critical infrastructure.



**TO DRIVE THE MOVE TO THE CLOUD, THE U.S. FEDERAL GOVERNMENT LAUNCHED THE "CLOUD FIRST" INITIATIVE IN 2011. IN 2019, THE GOVERNMENT UPDATED ITS GUIDELINES IN A REPORT CALLED "CLOUD SMART" TO ACCELERATE ADOPTION OF CLOUD-BASED SOLUTIONS.**

An ensuing "Report to the President on Federal IT Modernization" was submitted to the President later the same year. The report "outlines a vision and recommendations for the Federal Government to build a more modern and secure architecture for Federal IT systems." Its recommendations are grouped into two general categories: the modernization and consolidation of networks, and the use of shared services to enable future network architectures. The report "envisions a modern Federal IT architecture where agencies are able to maximize secure use of cloud computing [and] modernize Government-hosted applications."

In December 2017 the Modernizing Government Technology (MGT) Act was signed into law, providing funding mechanisms and technical expertise to help agencies implement security and modernization projects.

The notion of using cloud-based services is hardly new for federal government agencies. To drive the move to the cloud, the U.S. Federal government launched the "Cloud First" initiative in 2011. In 2019, the government updated its guidelines in a report called "Cloud Smart" to accelerate adoption of cloud-based solutions. FedRAMP is designed to help agencies rapidly evolve from aging, less secure legacy IT solutions to secure, cost-effective cloud-based IT.

Taken together, these developments incentivize public sector organizations to modernize quickly. Constituents want government agencies to provide new digital offerings mirroring those they see in the private sector, including online offerings that are secure, easy to use, and convenient. The Department of Defense (DoD) is also eyeing cloud services to ensure it does not miss out on the agility required to make warfare more effective and safer.

Signing on with a FedRAMP-authorized cloud provider gives agencies confidence that the vendor has taken appropriate steps to reduce security risks. FedRAMP compliance ensures a baseline, so agencies don't have to repeatedly certify services and can accelerate their authority-to-operate (ATO).

All cloud services used by U.S. federal government agencies must have FedRAMP authorization. Given its robust risk management framework, the program is also increasingly winning favor with state and local agencies as well as many in the commercial sector.

## **Modernization Challenges**

Of course, no law passed by Congress magically removes all factors that have been thwarting attempts to modernize government IT.

The aging workforce is one such factor. While agency IT staff have expertise with legacy infrastructure, they often lack the skills required to manage newer technologies. And with the level of sophistication of modern technologies, network environments, and deployment paradigms, this skills gap can hamper agencies in their drive to embrace innovation.

A second factor slowing modernization efforts is the lack of visibility into cloud platforms. Without access to monitoring and troubleshooting tools, including those that operate across multiple clouds, agencies are missing important metrics such as performance, uptime, and availability. It can also be difficult for agency IT groups to estimate levels of cloud resource usage, potentially leading to budget overruns.

THE U.S.  
GOVERNMENT  
ACCOUNTABILITY  
OFFICE (GAO)  
ESTIMATES  
**75%**  
OF AGENCY IT  
BUDGETS ARE  
SPENT OPERATING  
AND MAINTAINING  
EXISTING LEGACY  
IT SYSTEMS, NOT  
ON STRATEGIC  
EFFORTS.

The way in which many agency networks and systems grew—in a gradual, piecemeal fashion—presents yet another challenge. In many agencies, it's hard for any single IT professional to have a big-picture view of the current IT architecture. Without that, it's difficult to know what steps to take around modernizing the environment.

Agencies also lack clarity on what the business outcomes from modernization should look like, although the 2017 Federal IT Modernization Report does help address that issue with respect to cybersecurity goals. The report makes it clear that cybersecurity needs to be a priority and lays out a risk-based approach. "Agency heads will be held accountable by the President for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data." This means agencies need tools to perform continuous diagnostics and mitigation (CDM), including monitoring for unauthorized access and employing advanced threat detection techniques to combat cyber-threats in real time.

"The risks to government agencies' computing environments are in no way diminished strictly because the environment is in the public sector," says Bob Bragdon, senior vice president and publisher of CSO. "The same risks are faced by organizations globally, and the ever-increasing volume and scope of compliance regulations continue to present significant challenges."

### Cloud Adoption has Been Slow

Certification requirements are one reason government adoption of cloud services has been sluggish. But a more significant stumbling block is the nature of government IT environments. As noted above, agencies have accumulated various tools and solutions over the years that create multiple silos. It's a challenge to determine the exact components of any given service or application and understand which ones are relevant for migration.

It's also difficult to gain visibility across the entire environment, which makes it hard to determine how to migrate workloads to the cloud – and how to measure the required levels of performance and availability. (On a related note, visibility may continue to be an issue even after a cloud migration, given the need for multiple cloud providers).

“ The drive to move to the cloud has been tempered by the challenges of staffing, expertise, resources, and compliance mandates. But like in the private sector, **government agencies can realize significant benefits from moving operations to a cloud model**, including greater resiliency, flexibility, and cost savings. ”

— BOB BRAGDON, SVP AND PUBLISHER, CSO



**Armed with data-driven insights,** agencies can quickly make confident decisions and take decisive action.

---

Agencies are also contending with a looming skills and resource gap. Much of the government workforce is at or nearing retirement age, meaning valuable institutional knowledge will walk out the door.

Furthermore, the U.S. Government Accountability Office (GAO) estimates 75% of agency IT budgets are spent operating and maintaining existing legacy IT systems, not on strategic efforts. It can be difficult for leadership to spearhead migration efforts while simultaneously managing multiple, complex issues and ensuring current systems can continue to support the mission.

“Public sector challenges are not really that different from those in the private sector,” says Bragdon. “The drive to move to the cloud has been tempered by the challenges of staffing, expertise, resources, and compliance mandates. But like in the private sector, government agencies can realize significant benefits from moving operations to a cloud model, including greater resiliency, flexibility, and cost savings.”

## **New Technologies on the Horizon**

Adopting cloud technologies can not only open the doors to agility but also improve the effectiveness of services and internal IT operations.

A cloud-based, real-time data analytics platform can help accelerate modernization initiatives. It can also provide visibility into existing applications and metrics, allowing agencies to better understand what resources are being used and to what extent. This visibility can help plan appropriate levels of cloud resources and most importantly, ensure that usage is metered and unanticipated costs avoided. Such a cloud-based platform can also help agencies adopt the application rationalization practice encouraged by the U.S. General Services Administration (GSA) to trim costs and eliminate “redundancies in capabilities across business lines, the costs of infrastructure, and the required support and licensing associated with legacy solutions.”

# Cloud-based Data Analytics Can Help with Modernization Efforts

Staff- and budget-strapped agencies may have a difficult time taking on new cloud technologies on their own. But cloud providers can help in a variety of ways:



A FedRAMP authorized provider can **ease the security burden on agency IT staff**. FedRAMP authorization ensures adherence to a set of approved security controls that agencies can be confident about. This authorization accelerates agency authority to operate (ATO), while enabling proactive risk management from the start.



Cloud services let government IT groups access **state-of-the-art infrastructure and consolidate data center resources**, including eliminating time-consuming O&M activities.



Adopting cloud-based services will help agencies **better focus on their mission and tackle strategic initiatives**.



A cloud-based data analytics solution **drives insights so agencies can confidently make solid decisions and take action**.



An independent monitoring solution can help **eliminate blind spots by covering any deployment** — on-premises or cloud — bringing holistic visibility to gain quick, valuable insights across the mission.



With the ability to quickly spin up new workloads and applications in the cloud, agencies can **deliver new services faster, and with increased performance and reliability**; that leads to higher customer satisfaction and contributes to improved agency morale and reputation.

Additionally, by monitoring usage of various components that make up the applications or systems, IT departments can rationalize applications and migrate only the critical components, in turn reducing costs.

Experts offer these tips for agencies planning a move to the cloud:

- ▶ **Before a cloud migration:** IT should measure the baseline user experience and performance, and define acceptable post-migration levels. Degradation in one performance area may be acceptable if it's offset by gains in another. To accurately validate a migration's success, use the same monitoring tool throughout the migration process.
- ▶ **During cloud migration:** IT must closely monitor established performance metrics using a dashboard and alerts. Variation from the baseline is an early indicator of trouble; identifying issues well before production will save time and resources.
- ▶ **After a cloud migration:** The same monitoring solution can measure acceptable metrics and success. Continued monitoring is essential to ensure consistently high-quality customer experiences that cross on-premises and public cloud workloads.

## The Bottom Line

Government agencies can succeed in their modernization efforts. FedRAMP-authorized cloud services offer a solution, providing a viable avenue for agencies to quickly meet their needs with modern, secure, reliable infrastructure and applications.

The Cloud Smart initiative represents a studious approach, covering the elements that constitute proper security and how to overcome challenges around procuring cloud-based services. Cloud Smart includes significant guidance around workforce issues, such as identifying skills gaps, retraining existing employees, and recruiting and hiring. In short, Cloud Smart will help agencies harness the new capabilities cloud services offer and expand existing ones to deliver a quality customer experience.

**In addition, signing on with FedRAMP-authorized providers enables “agencies to adapt from arcane legacy technology to mission-centric and cost-effective cloud-based systems in a more rapid, consistent, and secure manner,” according to the OMB’s Office of the Federal Chief Information Officer.**

A cloud-based data analytics solution can help agencies take advantage of objective, data-driven insights; for example, modeling and predicting how initiatives will play out in order to deliver on intended outcomes. Granular, real-time monitoring can also significantly improve the odds of success and help avoid budget overruns caused by excess resource consumption, unexpected expenses, and inaccurate billing. Armed with data-driven insights, agencies can quickly make confident decisions and take action.

With multiple mechanisms and incentives in place, it's clear that now is the time for government agencies to get on board with cloud services—to both modernize and take advantage of newer technologies and paradigms to deliver exceptional citizen experiences, and to succeed in their missions securely and efficiently.

# Splunk Cloud Helps Accelerate Agency Modernization Initiatives



To ensure mission success securely and efficiently, public sector organizations are leveraging the Splunk Data-to-Everything platform, including all three branches of the U.S. government and all 15 cabinet-level departments. With Splunk Cloud, agencies can ingest data once and use that same data to address a variety of challenges across their organizations. With the insights gained from data analysis, agency personnel can make confident decisions and take decisive actions at speeds their missions demand. Also, Splunk Cloud meets FedRAMP risk management and security requirements at the moderate impact level, accelerating agency Authority To Operate (ATO) while enabling proactive risk management from the start.

“Our FedRAMP authorization serves as further validation of Splunk’s commitment to our public sector customers and our ability to power digital transformation across government. We can now offer a single solution capable of solving IT, security and mission challenges for agencies where confident, data-driven, decisive actions matter for the success of the mission,” Frank Dimina, vice president of public sector, Splunk.



**Splunk has given us the ability to gain better insight into our data. Previously our reliance on on-premise infrastructure and software limited how far we could take that data. Splunk Cloud FedRAMP opens new opportunities to use data to further our agency’s mission.**

MARQUES YOUNG  
SOC Manager, International Trade Administration  
US Department of Commerce

## Splunk Cloud delivers the capabilities of Splunk as Software-as-a-Service (SaaS) to ensure faster time to value, security and reliability.



### SERVICE EXCELLENCE

Splunk Cloud is operated by our Splunk experts. Allow the Splunk team assist the staff and help with the processes and systems required to run Splunk on-premises. Instead, focus your time on making confident decisions and taking decisive actions.



### MAXIMIZES VALUE FROM LIMITED RESOURCES

As a service, Splunk Cloud subscribers don’t need to provision or manage infrastructure.

Subscribers can focus their scarce and valuable resources on strategic initiatives and mission objectives rather than managing and maintaining infrastructure.



### FAST AND FLEXIBLE

Accelerate time to value in as quickly as two days. Expand your deployment with incremental capacity available within two days, retain data for 90 days by default and have your upgrades and updates handled for you.



LEARN MORE ABOUT **SPLUNK CLOUD WITH FedRAMP** AND HOW TO AGGREGATE, ANALYZE AND GET ANSWERS FROM YOUR DATA IN JUST DAYS.