

YOUR GUIDE TO

# Cloud Security in Government Today

Making the Most of FedRAMP



# Contents

3	Executive Summary	23	Making Government Cloud Safe With FedRAMP
4	Carahsoft's IT Solutions Providers Embrace FedRAMP	24	A Q&A With Guy Cavallo, Small Business Administration Deputy CIO
6	Cloud Security Today in Government – and How it Got Here	27	Cloud Security That's Built for Government Missions
11	The Fast Path to Hybrid Cloud for Government	28	What Are the Benefits of FedRAMP for Government?
12	A Q&A With Claudio Belloli, FedRAMP Program Manager for Cybersecurity	31	Adopting a Platform Approach for Cloud Security
15	Enhancing Your Digital Transformation Efforts With FedRAMP	32	A Q&A With Chris Cruz, California State Deputy CIO
16	Who and What Government Employees Need to Know About FedRAMP	34	A FedRAMP FAQ
19	Accelerating Threat Prevention in the Public Sector Today	35	Conclusion
		36	About & Acknowledgments

*Carahsoft and GovLoop have partnered to provide resources around the latest federal IT initiatives and legislation. The goal is to guide government leaders and stakeholders interested in learning more about procurement initiatives and the solutions available through them. We are proud to feature FedRAMP in our first-ever guide as agencies speed their cloud migrations and transition to Cloud Smart strategies.*

# Executive Summary

Government agencies have been talking about the cloud for more than a decade. With mandates from the White House like the Cloud First Policy enacted by the Obama administration in 2010 and, more recently, an updated approach to modernization as part of the 2018 Modernizing Government Technology (MGT) Act, as well as the shift to "Cloud Smart," the cloud has been a top-of-mind issue for agencies at all levels.

Security, however, was always the key sticking point for many agencies hesitant to move their systems into the cloud. Is the cloud secure? How can you fully capitalize on the cloud and ensure security to advance your agency's mission while respecting compliance and security?

In order to assuage fears and set standards for cloud security, the government created the Federal Risk and Authorization Management Program (FedRAMP). Launched in 2012, FedRAMP has played a key role in the adoption of cloud by establishing a common baseline for securing cloud products and services.

And agencies at all levels of government see the value in using standards to improve cloud security. Although FedRAMP is a mandatory federal program, there is a growing number of state and local governments using the same requirements to evaluate their cloud service providers (CSPs). The benefits include time and cost savings when verifying security practices at those companies, as well as a level of assurance that vendors have met rigorous security requirements.

Additionally, one of the biggest benefits FedRAMP provides is the ability for agencies to reuse and build on one another's work. Rather than each agency re-evaluating the same cloud services, they can share notes and ask questions to determine if those services meet their needs. The premise of FedRAMP is that the baseline standards it provides cover requirements that are common across agencies. That frees agencies up to focus on the few requirements that may be unique to them.
























"Individual agencies can accept their own level of risk associated with a cloud service when authorizing that cloud service (as allowed by the Federal Information Security Management Act), [but] one agency may be hesitant to reuse another agency's authorized cloud solution because it may not trust the risk tolerance associated with that authorized cloud solution," Ashley Mahan, FedRAMP Acting Director, told GovLoop.

In this guide, brought to you by GovLoop, Carahsoft and partner companies, we look at the current state of cloud in government, more specifically, the state of cloud security, the role of FedRAMP and how agencies can move forward with digital and modernization efforts securely.



## Carahsoft's IT Solutions Providers Embrace FedRAMP

More than 60 FedRAMP solutions are available through Carahsoft, enabling agencies across Federal, State and Local Government to access a wide range of cloud-based technologies to securely drive modernization and digital transformation.

 <b>Accellion</b>	Kiteworks Federal Cloud	 <b>CYLANCE</b>	CylancePROTECT
 <b>aconex</b>	Aconex Collaboration Platform for Project Information and Process Management	 <b>databricks</b>	Databricks FedRAMP Unified Analytics Platform
 <b>Acquia</b>	Acquia Cloud	 <b>DECISION LENS</b>	Decision Lens Software
 <b>Adobe</b>	Adobe Analytics Adobe Campaign Adobe Connect Managed Services (ACMS-GC) Adobe Creative Cloud for Enterprise Adobe Document Cloud (PDF Services & Adobe Sign) Adobe Experience Manager Manged Services (AEMMS-GC)	 <b>DocuSign</b>	DocuSign Federal
 <b>DOMA TECHNOLOGIES</b>	DOMA Software Platform	 <b>druva</b>	Druva inSync
 <b>AGARI</b>	Brand Protection	 <b>FRAME</b>	Frame Platform Government Edition
 <b>Akamai</b>	Content Delivery Services	 <b>FIREEYE</b>	FireEye Email Threat Prevention (ETP) Security Service
 <b>aws</b>	AWS GovCloud AWS US East/West	 <b>Google Cloud</b>	Google G Suite Google Service (Google Cloud Platform Products and underlying Infrastructure)
 <b>APPTIO</b>	The Apptio Technology Business Management (TBM)	 <b>GRANICUS</b>	GovDelivery Communications Cloud
 <b>AXON</b>	Axon Evidence.com	 <b>Hootsuite</b>	Hootsuite Enterprise
 <b>BlackBerry</b>	BlackBerry Cloud - AtHoc Services for Government	 <b>ivant</b>	Ivanti Service Manager
 <b>box</b>	Box enterprise Cloud Content Collaboration Platform	 <b>Lookout</b>	Lookout Mobile Endpoint Security
 <b>ca technologies</b>	CA Infrastructure General Support System CA Project & Portfolio Management (PPM)	 <b>MICRO FOCUS</b> Government Solutions	Fortify on Demand
 <b>CoSo Cloud</b> an AASKI company	CoSo Cloud FedRAMP Managed Service Platform		

 <b>McAfee</b>	McAfee MVISION Cloud	 <b>servicenow</b>	ServiceNow Service Automation Government Cloud Suite
 <b>MuleSoft</b>	Anypoint Platform - Federal Edition	 <b>slack</b>	Slack
 <b>netskope</b>	Netskope Security Cloud	 <b>Socrata</b>	Socrata Data Platform
 <b>New Relic</b>	New Relic	 <b>splunk</b>	Splunk Cloud
 <b>okta</b>	Identity as a Service (IDaaS)	 <b>springcm</b> A DocuSign Company	SpringCM
 <b>paloalto</b>	Palo Alto Networks Government Cloud Services - WildFire	 <b>Symantec</b>	Symantec Email Security Service - Government powered by Rackspace Symantec Cloud SOC Symantec Data Loss Prevention (DLP)
 <b>proofpoint</b>	Proofpoint Email Archive Proofpoint Email & Information Protection Service Proofpoint Target Attack Protection	 <b>TIBCO</b>	Tibbr
 <b>qualtrics</b> EXPERIENCE MGMT	Qualtrics XM Platform	 <b>VALIMAIL</b>	Valimail Enforce Platform
 <b>Qualys</b>	Qualys Cloud Platform	 <b>VERITONE</b>	aiWARE Government
 <b>rackspace</b>	Rackspace Government Cloud	 <b>virtru</b>	Virtu Data Protection Platform
 <b>salesforce</b>	Salesforce Government Cloud	 <b>virtustream</b>	Federal Cloud (VFC)
 <b>NS2</b> NATIONAL SECURITY SYSTEMS	SAP NS2 Cloud - SuccessFactors HCM Suite for Government SAP NS2 Secure Node with SuccessFactors Suite - DoD	 <b>vmware</b>	Airwatch by VM Government Services (AGS) Workspace ONE VMware Cloud on AWS GovCloud
 <b>SAVIYNT</b>	Identity Governance as a Service (IGAaaS)	 <b>workiva</b>	Wdesk
		 <b>zscaler</b>	Zscaler Internet Access - Government Zscaler Private Access - Government (VPN Replacement)

Carahsoft's FedRAMP solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ACCENT, NASPO ValuePoint, National IPA, and numerous state and local contracts. Learn more at [Carahsoft.com/FedRAMP](https://Carahsoft.com/FedRAMP)

# Cloud Security Today in Government – and How it Got Here

## The State of Cloud in Government

There were doubts about the practicality of cloud solutions when the Obama administration introduced the "Cloud First" strategy in 2010. Eight years later, the cloud is ubiquitous, and in 2018, the Trump administration announced the "Cloud Smart" initiative, a sequel to Cloud First that Federal CIO Suzette Kent said will build on federal cloud adoption.

With questions of cloud capabilities answered, however, new questions arise. Should government clouds be public, private or hybrid? What sorts of security updates are necessary before agencies can migrate to the cloud? How do agencies start to integrate cloud technology?

Answers vary from agency to agency. And yet, agency-specific solutions have been well regarded so far. Of the first six [Technology Modernization Fund awards](#) – loans to agencies to assist in costly IT modernization projects – three have focused on cloud migrations, totaling \$40 million. The Housing and Urban Development Department (HUD) is moving to a cloud-based application suite, the Energy Department is undertaking a massive enterprise cloud email migration and the Agriculture Department (USDA) is powering a shared services cloud platform model. Additionally, the new Centers of Excellence (CoEs) program, which HUD and USDA are the launch sites for, targeted cloud as one of five CoEs.

## The State of Cloud Security

As the cloud grows in prominence, so do security threats. More and more, malicious actors try to infiltrate government data – for personal or political gain – and have proved that government IT departments can't afford to be complacent. Cloud Smart encouraged agencies to move their security focus from mainframe and network protection to data protection. To best defend their assets, agencies have to adapt to modern-era capabilities, and cloud is the most secure way.

While the cloud is generally acknowledged as one of the most secure forms of application and data management, it didn't become that way overnight. To accompany new business potential, there needed to be new security measures and methodologies. "The perimeter is the person now," said Gregory Touhill, the first Federal Chief Information Security Officer and President of Cyxtera Federal Group, at the 2018 Symantec Government Symposium. One such methodology, Zero Trust, a security strategy tailored to cloud environments, emphasizes user identity – with authentication and authorization.

How do agencies wield the power of the cloud, expanding their reach while guarding their core assets? Here, FedRAMP is part of that larger picture – helping government find the tricky balance between mission achievement and security.

## FedRAMP by the Numbers

FedRAMP covers more than **5 MILLION ASSETS** of the world's largest cloud providers



and **1/3** of the world's internet traffic through its program

FedRAMP offers **4 security baselines** so government can match security to risk



**HIGH**  
421 controls



**MODERATE**  
325 controls



**LOW**  
125 controls



**LI-SAAS\***  
38 controls

*\*Tailored for Low-Impact Software-as-a-Service*

**150+**  
Cloud Service Providers

**100+**  
Agencies

**40+**  
Auditors

Agencies reuse FedRAMP authorizations an average of 6X, equaling

**\$130,000,000**  
in cost avoidance



## FedRAMP by the Numbers

**47%**

of senior government leaders feel that cloud governance is nonexistent

Source: [Deloitte](#)

**4.5%**

of agency data in the cloud is uploaded to FedRAMP-compliant services. That leaves the vast majority (95.5 percent) of agency data stored outside of approved services

Source: [Sky High Networks](#)

**3.3%**

of apps in use by the average federal agency are FedRAMP-compliant

Source: [Sky High Networks](#)

**\$10M**

is what larger agencies, such as the Justice Department, reap in cloud savings annually

Source: [The President's Fiscal 2018 Budget Proposal](#)

**20.6%**

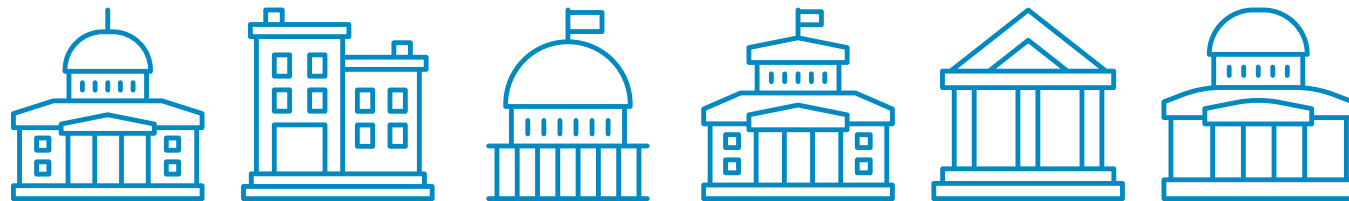
of local governments' IT budgets are spent on cloud

Source: [Gartner](#)

**22%**

of the national government's IT budgets are spent on cloud

Source: [Gartner](#)



To remain eligible for a Joint Authorization Board (JAB) provisional-ATO, a cloud system must have a minimum of six unique agency customers with authorizations to use the product or service.

Source: [FedRAMP](#)

## Timeline of Government Cloud Security Developments

### FEBRUARY 2010

Former Federal CIO Vivek Kundra announces a "governmentwide risk and authorization program for cloud computing" as part of the [25 Point Implementation Plan to Reform Federal IT](#).

2010

### FEBRUARY 2011

Kundra releases the Federal Cloud Computing Strategy, which makes the case for agencies to move to the cloud. It also details the [Cloud First Policy](#), which requires agencies to evaluate cloud options for new investments.

2011

### JANUARY 2012

Low and moderate FedRAMP security controls are released.

2012

### MAY 2012

The first Third Party Assessment Organizations (3PAOs) are accredited. GSA accredited nine: eight private industry organizations, and one government organization.

2013

### MAY 2013

The Health and Human Services Department issues the first agency ATO under FedRAMP.

2014

### JUNE 2012

FedRAMP launches.

2015

### JANUARY 2015

DoD announces cloud security requirements to build off of FedRAMP.

2016

### DECEMBER 2012

The Joint Authorization Board (JAB) issues the first FedRAMP provisional authorization.

2017

### OCTOBER 2018

The Office of Management and Budget (OMB) publishes its [Cloud Smart Strategy](#) proposal to provide more guidance around security, procurement and necessary workforce skills for cloud adoption.

2018



Migrating to the cloud? There's a new way forward.



2 proven leaders. 1 powerful platform.

VMware Cloud™ on AWS GovCloud (US)—a more perfect union.

With the combined power of VMware and Amazon Web Services—the industry-leading public and private cloud providers—VMware delivers a hybrid cloud solution designed to meet the unique needs of government, including time, budget, and security requirements.



**Strengthen security**

through a Zero Trust model that complies with FedRAMP certification



**Improve agility**

by working in a seamless hybrid environment, with nothing to rewrite or relearn



**Simplify operations**

for greater efficiency, faster migration, and additional CapEx and OpEx savings

Discover the ideal candidate for migrating government to the cloud:

[cloud.vmware.com/govcloud](https://cloud.vmware.com/govcloud)



INDUSTRY SPOTLIGHT

# The Fast Path to Hybrid Cloud for Government

An interview with Mike Wilkerson, VMware Cloud on AWS Specialist for Federal at VMware

Today, citizens using government services expect secure and user-friendly digital experiences, delivered any time, at any place, on any device. And the same is true about the government workforce. Employees need access to an increasingly complex IT environment in which connections and services are no longer fully managed by the agency.

To do this, more public sector agencies are moving their operations and applications to the cloud. And as they do this, agencies are looking to leverage a common cloud infrastructure, both on-premises and in the public cloud, to further increase agility and security.

To better understand how agencies can have a smooth, easy path when moving workloads to the cloud while staying secure and agile, GovLoop sat down with Mike Wilkerson, VMware Cloud on AWS Specialist for Federal at VMware, a leader in cloud computing and virtualization.

"Many of our federal customers are looking to get out of the infrastructure business," Wilkerson said. "They want to get out of the datacenter because they don't want to manage facilities. Today, they want a secure place in the hybrid cloud."

But agencies aren't necessarily shutting down all infrastructure, Wilkerson said. "Given the sensitive nature of

government data, they're not shutting down everything; there will still be a mix of on-premise infrastructure and cloud, with public vendor cloud use," he said.

VMware offers VMware Cloud on AWS GovCloud, a secure platform for government agencies to further increase agility and security by accessing the benefits of public and private clouds.

VMware has a long history of providing federal, state and local government agencies with software products that simplify the operation and management of IT. As part of its commitment to deliver technologies that help government operate more efficiently, VMware and Amazon Web Services, industry leaders in private and public cloud providers, announced VMware Cloud on AWS GovCloud back in June 2018.

VMware Cloud on AWS GovCloud is a jointly engineered, highly secure, scalable hybrid cloud service that brings VMware's software-defined data center software to AWS GovCloud. With the same architecture and operational experience on-premises and in the cloud, federal IT teams can now derive instant value from the use of the AWS and VMware hybrid cloud experience.

VMware Cloud on AWS GovCloud allows agencies to securely deploy a hybrid cloud solution by seamlessly extending their vSphere-based

infrastructures to AWS's global infrastructure while maintaining operational consistency and leveraging existing tools in use today.

"This is the easy button for agencies to get from on-premise to the cloud," Wilkerson said. "Agencies can have the assurance of security layers, availability, FedRAMP certification, and more."

*"Agencies today want to get out of the datacenter because they don't want to manage facilities. Today, they want a secure place in the hybrid cloud."*

**Takeaway:**

**As government agencies increasingly move workloads to the cloud, the ability to seamlessly integrate VMware software applications with AWS helps simplify the IT modernization journey for federal agencies.**

# A Q&A With Claudio Belloli, FedRAMP Program Manager for Cybersecurity

More than 150 agencies are using FedRAMP-authorized cloud services. Through FedRAMP and its more than 120 authorized products, agencies are able to leverage existing authorizations and work off of a common set of security standards, which allows them to consider more options when migrating to the cloud. This process not only improves access to innovative cloud products to help agencies execute their missions, but has collectively saved agencies more than \$200 million.

To learn more about how FedRAMP is evolving to meet modern cloud security standards and agencies' needs, GovLoop sat down with Claudio Belloli, FedRAMP Program Manager for Cybersecurity.

## GOVLOOP: What are you hearing from agencies in terms of their greatest cloud security challenges and needs?

**BELLOLI:** The No. 1 challenge agencies are facing is keeping pace with the ever-increasing demand for cloud and ensuring that proper security is in place. Agencies are seeking cloud for low-risk business functions, such as collaboration and video streaming, as well as cloud solutions supporting sensitive, mission-critical data that has been kept out of the cloud in the past. Agencies are looking to FedRAMP to help them meet their demand for cloud and to augment their security capacity when it comes to bringing new and emerging technologies into their agencies.

## GOVLOOP: Can you provide specific examples on how FedRAMP is working to address them?

**BELLOLI:** In FY18, FedRAMP focused on meeting agency demand by:

- Adding 40 new cloud services to the FedRAMP Marketplace
- Adapting our FedRAMP Connect process to be quarterly instead of twice yearly
- Building capacity at agencies through hands-on training of more than 250 agency information systems security officers, and thousands of people through our virtual modules
- Developing a new baseline – FedRAMP Tailored – which provides agencies with an opportunity to authorize cloud services holding low-risk data

In FY19, FedRAMP is focused on technology and learning in service of our customers – the year of TLC. From a technology perspective, FedRAMP will target new, innovative offerings for authorizations to expand our marketplace. From a learning perspective, FedRAMP will continue to enhance training, in terms of both content and ease of use. Finally, FedRAMP will continue to serve our customers by facilitating regular communications and creating feedback loops where we can gain stakeholder perspectives and address opportunities for improvement, which will continue to inform our work.

## GOVLOOP: What are you seeing in terms of FedRAMP adoption outside the federal government and at the state and local levels?

**BELLOLI:** FedRAMP has become the gold standard for cloud security – not just as an element of federal cybersecurity, but also by industry and state and local governments. We hear from vendors that about a third of state and local requests for proposal (RFPs) they are seeing include being FedRAMP-authorized as a procurement requirement for vendors, and the National Association of State CIOs (NASCIO) has discussed applying FedRAMP to state-level systems. Financial sector executives have also talked with FedRAMP about how that sector can better leverage FedRAMP to ensure their systems are as secure as possible.

## GOVLOOP: What's the status of FedRAMP's work on automating the authority to operate process?

**BELLOLI:** FedRAMP is partnering with National Institute of Standards and Technology (NIST) on the Open Security Controls Assessment Language (OSCAL) effort, which is focused on automating the ATO process through the development of machine-readable content (e.g., XML, JSON). FedRAMP plans to pilot this with a few vendors once this goes live. When it's fully implemented, vendors can significantly reduce their level of effort (LOE) to create, deliver and analyze documentation. This will also give FedRAMP the ability to increase throughput of vendors, bringing more cloud products to agencies.

## GOVLOOP: There have been talks about how to mature and automate more elements of the FedRAMP process. What types of things is the FedRAMP PMO considering? What would these changes mean for agencies (how would they benefit in the long run)?

**BELLOLI:** FedRAMP has implemented new processes that reduced the FedRAMP JAB authorization time by 75 percent – completing most authorizations in as little as three months – all without compromising security. We've also reduced the level of effort for vendors by simplifying documentation and better aligning them with vendor business processes, saving both time and resources.

FedRAMP is currently exploring how to implement automation more broadly through our FY19 TLC initiatives (e.g., OSCAL). This will expedite the process for both CSPs and agencies.



# Reimagine the government experience.

Only Adobe brings together data and content to deliver amazing government experiences. In 2015, Adobe received FedRAMP agency approval for its cloud services for government. In 2018, we became the first vendor to receive FedRAMP Tailored authorization for Adobe Creative Cloud for Enterprise and Document Cloud services.

Learn more at [adobe.com/government](https://adobe.com/government)  
To request a demo call 1-800-87 ADOBE



Adobe Experience Cloud

## INDUSTRY SPOTLIGHT

# Enhancing Your Digital Transformation Efforts With FedRAMP

*An interview with Jonathan Benett, Technical Director, Digital Government Solutions, Adobe*

IT modernization is a journey, not a destination, for federal agencies. It's a digital transformation that can improve an agency's cross-channel communications, business processes and web services for citizens. Cloud services keep this journey moving smoothly – but what happens when security slows down your progress?

In a recent interview with GovLoop, Jonathan Benett, Technical Director, Digital Government Solutions at Adobe, explained how using one set of cloud security requirements, such as FedRAMP, ensures your agency's digital transformation doesn't lose steam. Adobe is a leading provider of digital solutions to government agencies for improving the citizen experience.

Benett said that FedRAMP determines the cloud products and services capable of meeting your agency's cybersecurity needs.

"You're never done with innovation and security," he said. "Having cloud services in a FedRAMP environment makes it easier to adopt the advances in both."

Cloud, meanwhile, enables data analytics, electronic forms and signatures, web conferencing and other useful tools. Applications like these ultimately help agencies better serve the public.

"FedRAMP makes it easier to adopt these digital transformation solutions in an accredited environment," Benett said. "That environment has implemented, documented and tested a large collection of security controls that make it easier for IT organizations to then trust that their services are being delivered in a safe, secure and privacy-aware way."

Cloud's flexibility also means that it adapts to changes in security, services and technology. Secure cloud enables better citizen outreach, digital asset and rights management and web conferencing for agencies.

"All of the agencies that are pursuing digital transformation solutions can more quickly adopt them when they're delivered through the cloud," Benett said. "The alternative is updating the existing applications running in a data center and going through the security gauntlet again."

FedRAMP additionally enables secure digital and electronic signatures for agencies. Adobe's digital and electronic signature solutions let your agency respond faster and sign contracts with citizens quicker. Constituents, meanwhile, no longer need paper documents for signing forms.

"It's not just moving from paper to digital forms but making sure that those experiences are available on a wide variety of devices – smartphones, tablets, smart screens and home devices," Benett said. "It's also making sure that electronic correspondence and statements can be delivered securely online."

*"You're never done with innovation and security," Benett said. "Having cloud services in a FedRAMP environment make it easier to adopt the advances in both."*

### Takeaway:

**Programs like FedRAMP enable broader digital transformation such as improved cross-channel communications and modernized forms and web experiences.**



# Who and What Government Employees Need to Know About FedRAMP

## Who's involved in the FedRAMP process?



### Government Agencies

FedRAMP is a federally mandated program, but state agencies can apply the FedRAMP framework in their cloud contracts and assessments. State agencies, however, are not authorized to directly access FedRAMP security documentation housed in a secured, federal portal. Under FedRAMP, there are specific roles and responsibilities that agencies must assume.



### Cloud Service Provider (CSP)

CSPs that are interested in selling their cloud service to the federal government should obtain a FedRAMP authorization.



### Third Party Assessment Organization (3PAO)

3PAOs perform the initial and periodic assessments of cloud systems to ensure they meet FedRAMP security requirements.



### Joint Authorization Board (JAB)

The JAB is the primary governance and decision-making body for the FedRAMP program and is composed of chief information officers from the General Services Administration (GSA) and the Homeland Security (DHS) and Defense (DoD) departments.



### FedRAMP Program Management Office (PMO)

The FedRAMP PMO is situated within GSA. The PMO has several roles, including serving as the liaison between agencies, CSPs and the JAB, and providing program communication and outreach.

# AUTOMATED GLOBAL THREAT PREVENTION

WildFire®: U.S. Government malware prevention service has achieved FedRAMP In Process designation.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)



## INDUSTRY SPOTLIGHT

# Accelerating Threat Prevention in the Public Sector Today

*An interview with Tom Conway, Director, Federal Business Development, Palo Alto Networks*

Government today faces more adversary automation than ever. Not knowing where to start, government agencies often (erroneously) think hiring more people is the answer.

"Thanks to the growing automation of attacks, the volume, variety, velocity and complexity of threats are continuing to accelerate," said Tom Conway, Director, Federal Business Development, at Palo Alto Networks, a leader in cybersecurity products that use automation to prevent threats across networks, clouds and endpoints.

GovLoop sat down with Conway to better understand how agencies can reduce their cyber risk in cloud environments. Government continues to embrace cloud to reduce operating and maintenance (O&M) costs and to create services with more agility. Their data and applications often span different clouds and services.

How can government ensure effective security for cloud? Cloud security is a shared responsibility between the cloud provider and the agency. Providers offer only basic native security services and specific to only their cloud environment. This generally won't satisfy immediate or longer term requirements for multi-cloud, visibility, compliance and threat prevention. The outcome: limited visibility, increased operational overhead to configure and maintain security for each unique cloud environment, fragmented compliance and increased risk.

The good news: Agencies can extend threat prevention holistically across their cloud (private, SaaS, IaaS, and PaaS) environments with Palo Alto Network's swift, comprehensive malware analysis service, WildFire. WildFire is an advanced analysis and prevention engine for highly evasive zero-day malware and exploits. The cloud-based service employs a unique multi-technique approach that combines dynamic and static analysis and innovative machine learning techniques.

Using data and threat intelligence from the industry's largest global community, the service identifies first-time-seen threats, performs advanced analysis and immediately shares protections across the network, endpoint and cloud. The services ensure data privacy through flexible data collection options.

"We've turned the automation game around: using automation (not people) to fight an automated adversary," said Conway. "We're really using technology that practitioners often think is years off."

This automation reduces the load on already-taxed teams, swiftly addressing new threats in less than five minutes and saving significant time, reducing events per hour to which any analyst must respond. Security analysts can focus on what matters – the much lower number of the most sophisticated threats that require human intervention.

"When it achieves its impending final FedRAMP ATO milestone, WildFire

will be the only cloud-based malware analysis service certified for the federal government," said Conway. "The FedRAMP-ready status reaffirms our company's commitment to supporting our federal government customers in securely transitioning to public cloud services."

*"Government should not sacrifice visibility just because its data is sitting in a cloud provider's datacenter. In fact, agencies should insist on equal or better visibility at that point, because you can't manage what you can't see."*

### Takeaway:

**Agencies need to also work on thinking about security from the cloud – that is, harvesting power of the cloud to enhance security, not only of other clouds, but of things that are still on premise.**

## What is an ATO, and what does that process entail?

An Authority to Operate, or ATO, is a term you'll hear often when discussing FedRAMP. It means that a senior-level official at your agency, known as the authorizing official, has granted a CSP permission to operate its services or products on government systems. When an ATO is issued, it also means that official has assumed any risks that come with that cloud service.

ATOs are not unique to cloud services. All information systems in use across the federal government must receive an ATO in order to

process federal data. It's also worth noting that FedRAMP's JAB cannot issue an ATO. "Only your own agency has the authority to issue ATOs for systems that your agency uses or operates," according to FedRAMP.gov.

The JAB can, however, issue a provisional ATO (P-ATO), which is an initial approval of a cloud service provider's FedRAMP security documentation, known as an authorization package. Agencies can use the documentation associated with that P-ATO to issue a final agency ATO.

**If your agency wants to issue an ATO for a provider that is already FedRAMP-authorized, here are the steps you'll need to take:**

1. Conduct a risk analysis by reviewing the CSP authorization package
2. Determine if the risk posture is acceptable
3. Determine if the CSP needs to meet additional requirements for agency mission/business needs
4. Approve the CSP package for authorization
5. Issue an ATO for the CSP service/system
6. Send the ATO letter to the FedRAMP PMO at [info@fedramp.gov](mailto:info@fedramp.gov)

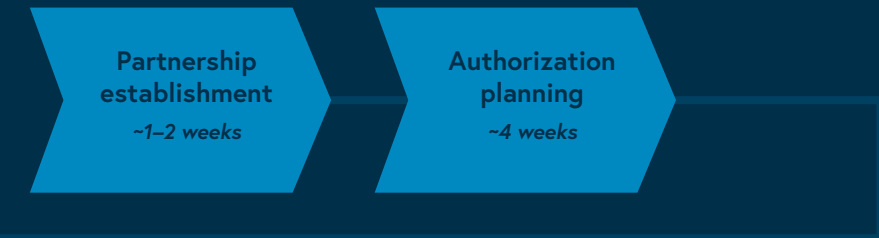
On the next page we've outlined what the process looks like if your agency wants to issue an ATO for a provider that is not FedRAMP-authorized. The FedRAMP Agency Authorization Playbook details each step in this process and outlines specific roles and responsibilities for your agency, the cloud service provider and the 3PAO.



## Process for issuing an ATO for a provider that is not FedRAMP-authorized

### 1. PRE AUTHORIZATION

Pre-authorization is where the agency, CSP and 3PAO collaborate in preparation for the agency authorization process.



### 2. DURING AUTHORIZATION

During authorization, the focus is on reviewing the cloud service offering security authorization package. The last steps in this phase involve providing the final approval of the cloud service offering's FedRAMP authorization package.



### 3. POST AUTHORIZATION

Post authorization is where an ongoing continuous monitoring process is established to ensure agencies are aware of current risks, vulnerabilities and changes to the cloud offering.



# Transform the Way You Secure Data and Deliver Services

Government data is filled with sensitive details about citizens, government spending, and national security. And that data spans countless agencies using different security strategies, in different clouds, with different standards. Meanwhile, cybercriminals are searching for opportunities. When they strike, agencies get compromised and the costs are steep.

While data stored in public clouds is exposed, data kept in U.S. government clouds is much more secure. Why? Because only organizations meeting approved federal security requirements have access to it. **And meeting those requirements takes the help of a FedRAMP-authorized cloud services provider like ServiceNow.**

**ServiceNow has undergone FedRAMP's rigorous vetting process.** The company also possesses a rare combination of expertise and experience. As a result, ServiceNow can help your agency achieve IT modernization goals, reach federal protection standards faster, and transform the way it delivers services.



Learn how ServiceNow can help you give your organization the data protection it deserves.

[www.servicenow.com/gov](http://www.servicenow.com/gov)

## INDUSTRY SPOTLIGHT

# Making Government Cloud Safe With FedRAMP

An interview with Mike Rohde, Deputy CISO, Federal, ServiceNow

The federal government's data is like a family's precious jewelry – it must be stored in a secure safe. Citizens' trust – and even well-being – can be damaged when agencies fail to protect this sensitive information and leave it vulnerable to people with bad intentions.

In an interview with GovLoop, Mike Rohde, Deputy Chief Information Security Officer, Federal at ServiceNow, explained how cloud security requirements like FedRAMP give your organization's data the protections it deserves. ServiceNow is a FedRAMP-authorized cloud services provider.

Rohde said that using FedRAMP standards as a guide, agencies can create a U.S. government community cloud, a model where every cloud consumer is on the same page with data storage, security and mission objectives. A U.S. government community cloud is a stamp of approval for federal agencies, promising that everyone involved meets FedRAMP's standards.

"The organizations that are allowed in a U.S. government community cloud must demonstrate that they meet particular requirements for protecting data and operate in specific regions," Rohde said.

Federal data often contains valuable information about individual citizens, government spending and national security. The cost of this knowledge falling into the wrong hands is

subsequently high. Today, many agencies put financial or citizen data into cloud environments, which means it is extra-sensitive and therefore deserves a safer storage place.

"If you're in a public cloud, you may be in the same environment as commercial customers that don't have the same stringent data requirements as a U.S. government community cloud," Rohde said.

Public cloud exposes federal agencies to risk from other participants who don't follow the same security standards they do. In contrast, a U.S. government community cloud only allows groups who meet the same federal requirements to interact with your agency's data.

FedRAMP, then, is an attractive rulebook for U.S. government community clouds. Any cloud consumer that follows FedRAMP's guidelines is reliable and secure for all federal agencies.

"FedRAMP's big benefit is that cloud providers like ServiceNow have gone through the rigor and due diligence to allow government consumers to use us," Rohde said. Additionally, it helps both public and private-sector participants reach federal security standards faster.

Another benefit is the ability for agencies to meet IT modernization goals. Cloud is a critical piece in modernizing federal IT. By using

cloud, agencies can transform the way they achieve their missions and deliver services to citizens. FedRAMP-authorized cloud offers agencies the confidence to leave their legacy IT behind without sacrificing their security. IT management services companies like ServiceNow help governments deliver faster, more reliable services to citizens.

*"The organizations that are allowed in a U.S. government community cloud must demonstrate that they meet particular requirements for protecting data and operate in specific regions."*

**Takeaway:**  
**FedRAMP is the foundation for U.S. government community cloud, a model where everyone involved meets the same data storage and security standards.**

# A Q&A With Guy Cavallo, SBA's Deputy CIO

The federal government has been testing a [workaround to the Trusted Internet Connections program \(TIC\)](#), an 11-year-old initiative to optimize and standardize the security of individual external network connections that federal agencies use.

The Small Business Administration (SBA) is one of the agencies leading that charge. But among the challenges that SBA's Deputy Chief Information Officer Guy Cavallo found was that TIC doesn't mesh well with cloud, and he plans to prove there are other options.

Under FedRAMP, TIC compliance is required. Cloud service providers must have an architecture that supports TIC, and agencies have to enforce TIC routing and compliance.

The security features SBA is testing are comparable to, if not better than what TIC provides, Cavallo said. For example, his team picked up on 13 attempted connections from Vietnam, a country where SBA doesn't maintain offices. As a result, the agency blocked those IP addresses from making future access attempts.

Cavallo appeared on a GovLoop online training in July 2018, shortly after wrapping up the agency's TIC pilot, to discuss cloud, security and modernization at SBA.

## GOVLOOP: Talk about how you're dealing with TIC and how that's going.

**CAVALLO:** Back in January 2018, OMB requested that agencies apply to do a TIC modernization pilot to see if there were any modernization alternatives after the last decade, other than doing the TIC like we've always done it. We jumped on that because as we've been implementing our SBA cloud and turning on our cloud security tools, we were blown away by what we were shown in the cloud and even more blown away when we pointed those security tools at our on-premise network and started setting off alarms left and right that our ongoing TIC, ongoing security operations center was not having the same alarms.

We were lucky enough to be one of three agencies selected to do the TIC, we were selected – each one had a different focus. Ours was on doing Infrastructure-as-a-Service in the Microsoft Azure commercial cloud, not the government cloud. We made the decision to go with the FedRAMP moderate commercial cloud because we did not have high-risk data at SBA, and it was a 90-day pilot. OMB, DHS and GSA all had representatives meet with us, we had a daily meeting with them, we showed them what we had already done with the cloud security tools and then we came up with the objectives, and really what we wanted to prove was: Could the cloud security tools give SBA the situational cybersecurity awareness and protection equal to or better than the TIC?

As we've tried to modernize the TIC in the past, it's been more of a checklist of here's the features and the controls that we did 10 years ago. How do we do that same control? We elevated the conversation beyond that. We said, 'Let's not look at it feature by feature, control by control. Let's look at the overall security awareness that it provides.' We had great participation from DHS. We ended up taking all of our network feeds, [and] all of our firewall feeds. DHS worked with us to get us their feeds, and we were able to build a set of dashboards that was

eye-opening as far as what we could see, from the desktop to the servers, whether they're in the cloud or not, we had incredible visibility.

We finished that pilot [in 2018]. We think it was a very big success. We're in the middle of finalizing our report and our recommendation to OMB for that, which I know they will consolidate with the other two agencies, and I definitely think it's going to have an impact on the future OMB directives for TIC and cloud. Overall, we've had several meetings with Suzette Kent, the Federal CIO. We've shown this to her, and I can tell you, I sleep a lot better at night now that I have these cloud security tools protecting me than I did when I depended on my standard, regular government security operations center and the traditional TIC.

## GOVLOOP: You're able to provide better services and get more data through there, so your employees are happier and you haven't sacrificed security, right?

**CAVALLO:** Right. We're definitely seeing a performance boost by not having to go through the TIC, and we were given an exemption for going through the TIC to prove this project. In fact, at the end of it, we had to go back and plug the TIC back in so we could measure the impact of going through the TIC, and that was a little weird and we've definitely seen a performance hit, but even more important than that performance hit, the level of security protection that I'm able to see, we're being told things that are not even close to being part of the TIC.

If I have a server in my enterprise that has the password or the username as the same name as the server name, that shows up as a red box with that answer pointing us at the server. We wanted to elevate it to security awareness and those are things that the TIC would not do. The TIC is just looking at traffic, and this umbrella is looking at many, many other features, such as improper or inadequate passwords on your servers.

*"I sleep a lot better at night now that I have these cloud security tools protecting me than I did when I depended on my standard, regular government security operations center and the traditional TIC."*



# Cloud Security Built for Government Missions

AWS was the first major cloud provider to achieve the US government's FedRAMP compliance standard, and was the first to be granted authorization for FedRAMP High workloads.

Learn how AWS can help speed your path to ATO.

Learn more: FedRAMP in AWS GovCloud  
Get started on your path to ATO.  
Contact the AWS Partner team at [ATOonAWS@amazon.com](mailto:ATOonAWS@amazon.com)

## INDUSTRY SPOTLIGHT

# Cloud Security That's Built for Government Missions

*This was written in partnership with AWS.*

There was a time when most agencies shied away from putting their data in the cloud. Skeptics questioned whether cloud-based systems could meet government requirements and how they could verify those claims, especially if they couldn't see or touch physical hardware.

But efforts such as FedRAMP have helped to ease those concerns by providing baseline requirements for securing cloud products and services in a standard way. Using FedRAMP as a guide, agencies still must determine which cloud systems best support their mission. GovLoop and AWS partnered to highlight what secure cloud vendors like AWS have to offer agencies that want to take a thoughtful, mission-focused approach to cloud adoption.

For agencies, security classification has been one of the biggest barriers in moving to the cloud.

Security requirements for data, applications and workloads greatly dictate where those things may reside and run. In June 2016, AWS became the first cloud service provider to receive authorization to support FedRAMP High workloads. The "High" designation means that any loss of confidentiality, integrity or availability of the data in that system could be expected to have a severe or catastrophic effect on organizational operations, assets or individuals.

Companies that meet the FedRAMP High baseline are deemed secure enough to host Personal Identifiable

Information, sensitive patient records, financial data and other Controlled Unclassified Information in the cloud. "The cloud on its weakest day is more secure than a client-server solution," said Sean Roche, Associate Deputy Director of Digital Innovation, CIA. "It's been nothing short of transformational. It has transformed our ability to build new capabilities."

The creation of FedRAMP requirements to secure high-impact systems was a major milestone not only for cloud service providers like AWS but also for government agencies. The reason? Federal agencies wanted to take advantage of the benefits of secure commercial cloud — even for mission-critical systems. They wanted the ability to quickly adapt to varying workloads and to only pay for the IT services they use.

Offerings like AWS GovCloud (US) provide agencies compliance without compromise by delivering a secure environment to run sensitive government workloads. Currently, agencies are using AWS GovCloud to power various innovative projects, including analyzing data on social media to collect information on adverse drug effects and collecting images from Mars.

For agencies that aren't quite ready to put high-impact systems in the cloud, AWS is also authorized to secure moderate-impact systems. Moderate-impact systems account for nearly 80 percent of cloud applications that receive FedRAMP authorization,

according to FedRAMP.gov. For agencies, this means they can tailor the appropriate level of security to each system, based on its classification. Both agencies and vendors can save time and money by taking advantage of an existing AWS provisional authority to operate (P-ATO) from FedRAMP's Joint Authorization Board.

As agencies move more workloads into the cloud, investing in offerings that further their mission in a secure, cost-effective way is key.

*AWS's FedRAMP High authorization, which includes over 400 security controls, gives U.S. government agencies the ability to leverage the AWS Cloud for highly sensitive workloads.*

### Takeaway:

**Security requirements for data, applications and workloads greatly dictate where those things may reside and run. That's why agencies need secure cloud solutions that are designed to support their mission.**

# What Are the Benefits of FedRAMP for Government?

*FedRAMP is critical for government agencies and users. Here's what you need to know about how it can benefit you and your agency.*

## FedRAMP is a big deal:

The program is mandatory, and federal agencies must ensure the cloud solutions they use meet FedRAMP requirements. FedRAMP uses a "do once, use many times" framework for vetting the security of cloud services. The program saves government an estimated 30-40 percent in costs, as well as time and staff resources.

## FedRAMP is the future:

Cloud computing is the way of the future for government agencies, and FedRAMP will play a key role. The program is credited with helping to accelerate government adoption of secure cloud solutions. Some state governments are also requiring adherence to FedRAMP requirements.

## FedRAMP levels the playing field:

Choosing the right cloud service for your agency can be challenging, but FedRAMP provides a baseline for you to compare the security of all potential vendors. The number of FedRAMP-compliant solutions has grown since the program launched in 2012.

## FedRAMP helps with IT modernization:

FedRAMP enables agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure and cost-effective cloud-based IT. It created and manages a core set of processes to ensure effective, repeatable cloud security for the government. It also established a mature marketplace to increase utilization and familiarity with cloud services while facilitating collaboration across government through open exchanges of lessons learned, use cases and tactical solutions.

## FedRAMP offers support:

According to FedRAMP.gov, "FedRAMP is an example of a true partnership between the public sector and industry; there are over 120 Federal Agencies and 160+ industry partners actively engaged with the program. It is one of our priorities to support Agencies and their journey to innovate, modernize, save time and money, and protect citizen data using the latest cloud technologies. We are here to assist and guide Agencies through the FedRAMP authorization process, as well as promote collaboration across the federal government."

## FedRAMP is also supporting agencies to:

1. **Provide high-level education** about the cloud, security and the FedRAMP program.
2. **Standardize the documentation and review process.** FedRAMP encourages agencies to perform their due diligence in reviewing all security documentation that is located within the FedRAMP secure repository prior to issuing an authorization.
3. **Clarify the risks that the authorizing agency accepted.** FedRAMP applies safeguards to ensure agencies are well informed prior to reusing an agency-sponsored ATO. The FedRAMP team reviews each sponsored agency-standard ATO package and provides a summary report (three to four pages) outlining the system risk to ensure each agency makes an informed review and decision. FedRAMP retains a copy of all authorized cloud service providers' security documentation and assists agencies in performing their due diligence in reviewing all security documentation.

## Some other benefits for government that FedRAMP offers:



Increases reuse of existing security assessments across agencies



Saves significant cost, time and resources by using a "do once, apply many times" strategy



Enhances transparency between government and cloud service providers



Provides a uniform approach to risk-based management



Improves real-time security visibility



Ensures consistent application of existing security practices



Increases confidence in security assessments



Increases confidence in security of cloud solutions



Increases automation and near real-time data for continuous monitoring

# Salesforce is for Government

The world's #1 CRM connects people, data and technology

Learn more at [Salesforce.com/government](https://Salesforce.com/government)

## INDUSTRY SPOTLIGHT

# Adopting a Platform Approach for Cloud Security

*An interview with Paul Tatum, Vice President, Systems Engineer for the Public Sector Unit, Salesforce*

Government has a remarkable opportunity to modernize technology infrastructures to meet the needs of today's digitally savvy users. By pivoting to meet these new demands, agencies are able to open up new government services and new channels of connecting, while streamlining their IT programs and saving taxpayer dollars.

Moving to the cloud is one way agencies are transforming. But as different instances of cloud get set up across agencies, siloes are created, and a holistic approach to security can become nearly impossible.

To better understand how using a cloud platform approach can help agencies keep their clouds secure, GovLoop sat down with Paul Tatum, Senior Vice President, Solution Engineering for the Public Sector Business Unit at Salesforce. Salesforce is a leader in cloud-based customer relationship management (CRM) platforms.

Tatum described handling cybersecurity in government like a game of whack-a-mole for CIOs and CISOs. "Today, because of legacy technology and infrastructures, agencies are faced with many different siloed systems requiring lots of time, attention, and expense," he explained. "If a security directive comes out, it is very hard to comply with it holistically. Agencies are attempting to patch, remediate and scan across an impossible combination of legacy systems, technology, software versions."

This is challenging as the time spent dealing with security in a reactive way means agency IT teams may not be able to work towards meeting mission need.

While government needs to stay secure and compliant, they must also be able to innovate, optimize cost and stay agile in their approaches and development. Setting up an enterprise cloud platform can allow for more freedom, agility and compliance that government needs, while allowing them to leverage and inherit the built-in security and compliances.

One such platform is the Salesforce FedRAMP-authorized Government Cloud. It's a partitioned instance of salesforce.com's multitenant public cloud infrastructure, specifically for use by federal, state, and local government customers. It enables organizations to digitally transform the business of government rapidly and revolutionize the citizen experience, all while meeting the regulatory and compliance needs of government.

"We help agencies modernize with our integrated, secure cloud platform, which enables government to cut costs, accelerate mission success and provide a more complete ecosystem for employees, stakeholders and beyond," said Tatum. Salesforce's multitenant platform reduces security risks to agencies because their information is managed through a rigorous security monitoring and remediation program aligned with FedRAMP.

"A platform approach can truly be a gamechanger for government cloud security," Tatum concluded.

*"Using a multitenant architecture gives agencies a "single code base" platform. This allows everybody on that platform to instantly get the security and operational benefits that come as part of our FedRAMP authorization. This includes regular vulnerability scanning, remediation and reporting, all which are critical to delivering the secure, compliant applications that are vital to digital modernization".*

### Takeaway:

**Agencies should adopt a cloud platform approach, which allows them to leverage and inherit built-in security and compliance while accelerating their digital transformation efforts.**



# A Q&A With Chris Cruz, California Deputy State CIO

California ranks among the world's largest economies, so protecting its data is critical. FedRAMP offers the Golden State cloud cybersecurity standards that are worthy of America's national government.

California's state and local governments are now shielding their IT with different FedRAMP levels depending on their needs. In October 2018, the California Department of Technology's (CDT) CalCloud program began offering FedRAMP Moderate after long providing FedRAMP High services.

In this Q&A, California Deputy State CIO Chris Cruz, who is also CDT's Chief Deputy Director, explains how FedRAMP is strengthening California's cloud security.

## GOVLOOP: How is FedRAMP Moderate going to impact CalCloud and California's agencies?

**CRUZ:** Certain agencies qualify their data, usually by putting it into critical data categories. There's high, which means that you better have the highest levels of security around the cloud environment that you put that data in. Not everybody qualifies their data as high-risk, and so some think that there's medium risk. Having FedRAMP Moderate means that they still have FedRAMP protections, but it's not at the highest levels because they don't need those. Finally, there are other services that local governments have where it doesn't require FedRAMP Moderate or High. They just want to be able to buy commercial cloud services for things like their websites. They're buying for those assets that are a lower data risk.

Our new contract vehicle codifies and then gives them the option to purchase all those services. The previous contract only allowed them to buy FedRAMP High. We now have cloud services for low, medium and high-risk data qualifications. I call it the restaurant mentality. You go into a restaurant, and there are many things off the menu that you can now order for commercial cloud services and different data classification levels.

It's huge because this contract allows cities, counties and other regional offices to buy directly through CDT. That's significant, as that wasn't a part of the original FedRAMP High offering. The point is that we continue to mature our cloud offerings, and now we're offering these services to all government entities, not just the state ones. All of them can take advantage of discount pricing and a common security posture across California. We'll also do the procurements for them to provision into these cloud environments. That's huge, as a lot of cities and smaller counties don't have mature procurement organizations. Sometimes it takes them weeks or months to do these procurements with these cloud providers.

## GOVLOOP: What's the difference between FedRAMP High and FedRAMP Moderate?

**CRUZ:** It's how different agencies qualify their data. For example, there might be certain systems that different agencies maintain that have protected health information (PHI) or personally identifiable information (PII) data in it. If they're interested in migrating that application to the cloud, they're going to want FedRAMP High services. Because it's PHI, PII or something similar, they're going to

want to put their data in that level, as it meets the highest FedRAMP standards.

FedRAMP Medium says that you don't have PHI or PII data, it's not high risk and maybe you still want to take advantage of some of FedRAMP's moderate security offerings. You want to ensure that your data has some level of FedRAMP modification to it because that's the highest security standards to put your non-mission critical data in.

Most government entities are interested in migrating their applications into the cloud today. We've given them a standardized approach into what we call the government commercial cloud. It's standardizing California's IT infrastructure, which we're trying to do inside the state, with a common security posture and approach.

## GOVLOOP: Why would you want to comply with FedRAMP as a state or local government?

**CRUZ:** It's the security controls that give you ease of mind. If you're going to put your applications in an Infrastructure- or Platform-as-a-Service (IaaS or PaaS) cloud, it's that you have the highest levels of controls available to you that are in place in this cloud. That should allow you to sleep better at night, knowing that there's a certain amount of compliance that comes with FedRAMP. Given all the cybersecurity threats that we see on a continual basis, an ounce of prevention's worth a pound of cure.

## GOVLOOP: How would complying with FedRAMP impact California's relationship with the federal government?

**CRUZ:** I think we have a good relationship. We've adopted FedRAMP High and Moderate requirements as part of our security strategy. We have critical data here in California – we're the fifth largest economy in the world. We've got to aspire to the highest level of security standards there are, and FedRAMP provides that.

*"Given all the cybersecurity threats that we see on a continual basis, an ounce of prevention's worth a pound a cure."*

# FedRAMP FAQ

Hopefully by now you've gotten a good sense of what FedRAMP is, why it matters to you and where it's going in the future. But just in case you have a few more questions, FedRAMP.gov offers up a robust FAQ section, and we've taken some of its answers to its most frequent questions and included them here for your further understanding.

## What is the difference between FISMA and FedRAMP controls?

Both FedRAMP and FISMA use the NIST SP 800-53 security controls. The FedRAMP security controls are based on NIST SP 800-53 Revision 4 baselines and contain controls above the NIST baseline that address the unique elements of cloud computing.

## Who are the authorized FedRAMP approvers for federal agencies?

The FedRAMP approver to sign off on your Package Access Request form is either your agency's Chief Information Security Officer (CISO) or Designated Approving Authority (DAA). If the form is signed by a DAA, that person must be at a level that has the authority to grant an ATO for a system. Unfortunately, FedRAMP does not keep a listing of agency CISOs or DAAs. You will have to get that information from your agency.

## If an agency purchases an outsourced service (software) that is built on top of a cloud platform, how is that handled within FedRAMP?

Obtaining a FedRAMP authorization requires all system components be assessed based on the control requirements in the FedRAMP baseline. If a FedRAMP-authorized IaaS is leveraged, the agency only needs to assess controls that are not addressed by the managed IaaS provider. If a SaaS is hosted on a FedRAMP-authorized IaaS, the SaaS vendor would need to have a separate FedRAMP authorization. The IaaS authorization would remain as-is and then the SaaS would leverage/reuse the

IaaS authorization and applicable security controls (for the IaaS portion of requirements). If a SaaS or PaaS is leveraging a non-FedRAMP-authorized infrastructure, then the entire FedRAMP stack would need to be authorized together.

## Are third-party vendors required to be FedRAMP-authorized?

Depending on the services being offered, the third-party vendor does not necessarily have to be FedRAMP-compliant, but there are security controls you must make sure they adhere to. If there is a connection to the third-party vendor, they should be listed in the system security plan in the interconnection table. You can also search through the system security plan template and search on "third-party" or "third party" and see all of the security controls that apply to third-party vendors. Talk to your authorizing official to determine how best to handle third-party vendor offerings.

## Who will do the continuous monitoring and ongoing authorization of the cloud systems that have been authorized by an agency?

As a part of the FedRAMP requirements, federal agencies must implement a continuous monitoring program for any cloud system they deploy. FedRAMP requirements for continuous monitoring work to coordinate ongoing security across CSPs and agencies in accordance with DHS policies and guidance. However, agencies have ultimate responsibility for the continuous monitoring and ongoing authorization of the systems they use.

# Conclusion

The White House's modernization efforts are accelerating agencies' moves away from legacy systems. Additionally, citizens are demanding a new way of interacting with the government that is not effectively supported by outdated legacy systems.

Agencies that are not undergoing a digital transformation risk becoming stale and outdated. The way forward for governments is with cloud services. If leveraged in a strategic and prioritized way, the cloud allows agencies to properly take advantage of this transformational moment. And FedRAMP is enabling agencies across federal, state and local governments, to safely access a wide range of cloud-based technologies while remaining secure and compliant.

Not only can FedRAMP provide enhanced security and efficiency in the cloud as well as cost savings, but it also paves the way for agencies to reap the benefits of true digital transformation.

As agencies move further into the cloud, FedRAMP will help them stay secure as they continue on their path toward better digital services and modernizations that will serve the needs of citizens.

## About Carahsoft

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its best-of-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit [www.carahsoft.com](http://www.carahsoft.com), follow @Carahsoft, or email [sales@carahsoft.com](mailto:sales@carahsoft.com) for more information.

## About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to [info@govloop.com](mailto:info@govloop.com).

[govloop.com](http://govloop.com) | [@govloop](https://twitter.com/govloop)

## Thank You

Thank you to Adobe, Amazon Web Services, Carahsoft, Palo Alto Networks, Salesforce, ServiceNow and VMWare for their support of this valuable resource for public sector employees.

## Authors

Nicole Blake Johnson, Managing Editor













Catherine Andrews, Senior Director of Editorial and Production

## Designer

Kaitlyn Baker, Creative Manager

## Carahsoft's IT Solutions Providers Embrace FedRAMP

More than 60 FedRAMP solutions are available through Carahsoft, enabling agencies across Federal, State and Local Government to access a wide range of cloud-based technologies to securely drive modernization and digital transformation.

Carahsoft's FedRAMP solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ACCENT, NASPO ValuePoint, National IPA, and numerous state and local contracts. Learn more at [Carahsoft.com/FedRAMP](http://Carahsoft.com/FedRAMP)

*Carahsoft's FedRAMP solutions are available through its reseller partners on a variety of contracts including Carahsoft's GSA Schedule 70, SEWP V, ACCENT, NASPO ValuePoint, National IPA, and numerous state and local contracts. Learn more at [Carahsoft.com/FedRAMP](https://Carahsoft.com/FedRAMP).*

*See the latest innovations in government IT from Carahsoft's vendor partners at [Carahsoft.com/Innovation](https://Carahsoft.com/Innovation).*



1152 15th St. NW Suite 800  
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

[www.govloop.com](https://www.govloop.com)

@GovLoop