GOVFORWARD™

FedRAMP Technology Playbook

A guide to leveraging FedRAMP Policy and Technologies

Sponsored by: carahsoft.

Table of Contents

Scan Here

To learn more about what FedRAMP solution is right for you.

Introduction

The cloud is an almost unmatched enabler for government agencies. From digital government to artificial intelligence, tapping into the cloud gives agencies the tools they need to innovate effectively. And as agencies look for new ways to meet the mission, cloud adoption is only set to grow: Global government cloud market is set to more than double in the next five years. Moreover, Gartner predicts that, in order to improve resilience and agility, more than half of U.S. agencies will migrate critical applications to the cloud by 2025.

The Federal Risk and Authorization Management Program (FedRAMP) was established to help ensure that agencies are able to migrate workloads and data securely to the cloud.

But what is FedRAMP, how can agencies tap into it most effectively and what do different FedRAMP-authorized vendors have to offer? In this playbook, we answer those questions and more.

To learn more about what FedRAMP solution is right for you, reach out to FedRAMP@carahsoft.com.

Securing the Cloud: Why FedRAMP Is Critical to the Future of Agency Security

FedRAMP provides a regulated approach to security authorizations for cloud providers looking to service government agencies as they adopt cloud computing at an accelerated pace. At Carahsoft's GovForward Event, government and industry experts discussed FedRAMP's impact on the future of agency work, how certified cloud is serving their respective missions at scale, and how state and local governments are following suit.

It was not long ago that cloud computing was a relatively new business model in government. Few agencies bought IT services, and many struggled to grasp the logistics of cloud procurement, implementation and security. But in 2012, that all began to change with the launch of the Federal Risk and Authorization Management Program, commonly known as FedRAMP, a regulated approach to security authorizations for cloud providers looking to service government agencies.

Now, as agencies adopt new technologies and transition to the cloud at an accelerated pace, these streamlined security measures are more important than ever.

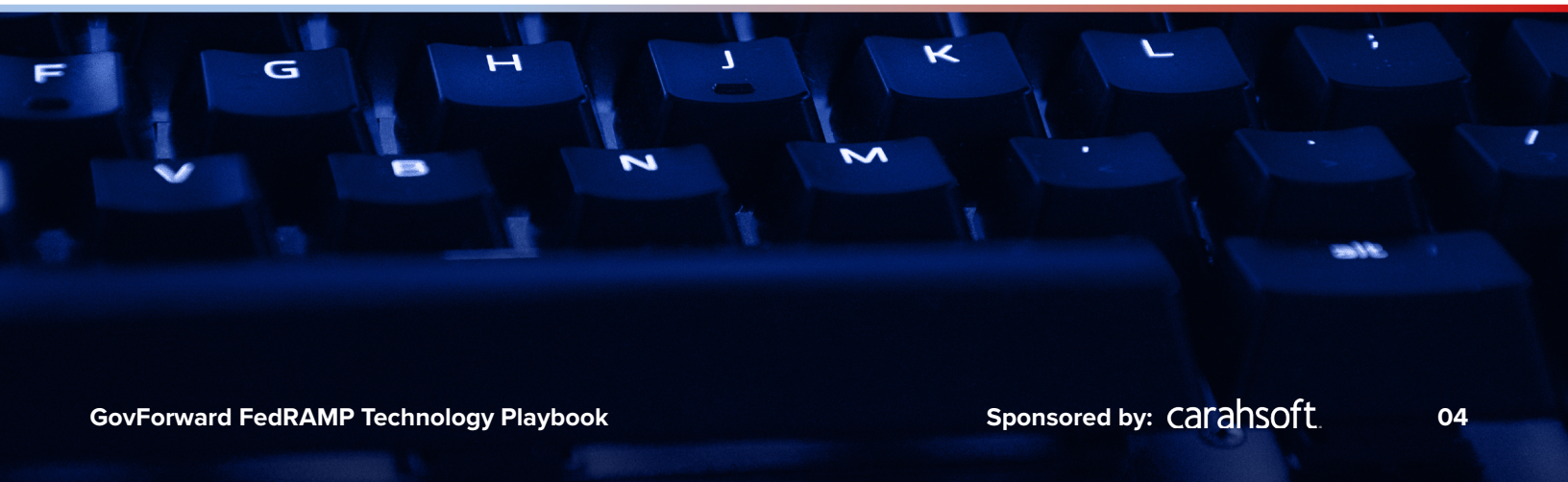
At Carahsoft's GovForward Event, government and industry experts discussed FedRAMP's impact on the future of agency work, how certified cloud is serving their respective missions at scale, and how state and local governments are following suit.

Here are a few key takeaways from the discussion:

1. Finding Common Ground

As agencies work to shift their on-premise applications, data and workloads to the cloud, they may not all use the same cloud provider. FedRAMP establishes a common baseline in MultiCloud environments for securing these cloud products and services before they are implemented.

"A common framework like FedRAMP provides guidelines that offer a holistic, repeatable methodology that helps organizations both understand and manage risk in the cloud," said Victoria Yan Pillitteri, acting manager of the security engineering and risk management group with the National Institute of Standards and Technology.



Pillitteri also noted that FedRAMP's risk-based architecture creates a common language between agencies to communicate cybersecurity risk management outcomes — how to understand, address and combat cyber threats in a unified way.

"A customary taxonomy is foundational because risk is incredibly subjective, my risks may be very different than my colleagues at other agencies serving different missions," she said. "So it's incredibly important for us all to speak the same language. If we're talking past each other, the core threats won't be addressed."

2. Security at Scale

Of course, cloud computing must be adopted at scale to meet the growing and shifting needs of hybrid and remote work environments — but it must be secured at scale, too. According to Department of State Deputy Chief Information Officer of Cyber Operations Al Bowden, as agencies continue to work together to develop a common security framework and language through FedRAMP, they will be able to create a scalable joint security and verification platform that can be leveraged across all government agencies. "Regardless of the agency's specific DNA, it is important to verify that underlying critical security controls are in place in measurable turnkey fashion," he said. "FedRAMP is bringing to bear this validation of solutions for all of government."

Lou Charlier, deputy chief information officer at the Department of Labor, added that once a cloud vendor is FedRAMP certified, they will have the authorization to improve the security of agency data and services hosted in the cloud.

"FedRAMP authorized offerings will become more attractive to agencies, and our cloud partners have an increased responsibility to share vulnerabilities and breaches with us as a federal partner, as well," he said.

3. FedRAMP's Impact on Defense

Still, FedRAMP's goal of tighter cybersecurity shouldn't compromise software modernization. Rob Vietmeyer, the director of cloud and software modernization for the Office of the Deputy Chief Information Officer at the Department of Defense, states that the DoD is at a critical junction as it strives to deliver better software at a much greater speed to warfighters while ensuring the utmost security.

"We are working to incorporate the next generation of cloud information technology for the warfighter, including streamlining data flows with complex tools like AI and machine learning for advantage in battle," he said, explaining that the first step in implementation is an effective, agile security foundation.

Through its standardized security framework, FedRAMP provides reusable cybersecurity control packages that cloud vendors can deliver quickly to keep pace with the DoD's valuable but fast-moving practices.

Vietmeyer stated that this accreditation allows DoD staff to rest assured that all products and tools they deploy are verified and secure at the start, leaving more room for innovation.

"When we look at how we are delivering mission value, it seems like everything's moving very fast or moving applications daily, or multiple times a day sometimes," said Vietmeyer. "But it's all because we have this security inheritance from FedRAMP being delivered by other parties at the start."

4. RAMPing Up Security for State and Local Sectors

While the federal sector optimizes FedRAMP, state and local governments must also adopt a security fabric that safeguards citizens' sensitive data in the cloud. Their solution was StateRAMP — launched in 2021 to enable state and local governments to reduce cyber risks and benefit cloud service providers by creating a "verify once, use many" approach.

"StateRAMP is designed to help states and local governments manage risk by verifying their suppliers' cybersecurity," said StateRAMP Executive Director Leah McGrath.

McGrath explains that the program audits and verifies vendor offerings and provides insight for local agencies to ensure products meet the minimum security requirements. Vendors who serve multiple states only have to go through the process once, rather than having to verify multiple times for each state.

“The real benefit and value to the providers is that they verify once in order to serve many,” she said. “By doing that collectively, we have the opportunity to work together to really improve cybersecurity, and raise our game in continuous monitoring and continuous improvement.”

5. Securing States to Protect the Country

Looking forward, StateRAMP is poised to work with federal partners to develop guidance that will drive more alignment between each state’s security frameworks.

“We are going to see a continued momentum and standardization of these best practices that can have a major and positive impact for efficiencies and state and local government, as well as for the providers,” said McGrath.

Streamlining and improving cybersecurity across states and local governments with StateRAMP will ultimately contribute towards the overall goal of bolstering the nation’s cybersecurity.

“Hopefully in the future StateRAMP will be implemented across all the states,” said Nancy Rainosek, chief information security officer from the State of Texas. “Especially now with cyberattacks on the rise, having unified security like this for every part of our country is very important.”

Watch the full event here.

HyperScaler Cloud Providers

Describe Your FedRAMP Solution

Amazon Web Services offers a broad set of global cloud-based products including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications: on-demand, available in seconds, with pay-as-you-go pricing. From data warehousing to deployment tools, directories to content delivery, over 200 AWS services are available. New services can be provisioned quickly, without the upfront fixed expense. This allows enterprises, start-ups, small and medium-sized businesses, and customers in the public sector to access the building blocks they need to respond quickly to changing business requirements.

What Challenges Does Your Solution Address?

AWS is a leader in the cloud computing field in addressing common challenges such as:
IT Focus I High Costs I Limited Access
Old Technology I Poor Business Continuity
Rigidity I Complicated Environment
Poor Communication I Use of Time I Risky Security

AWS is able to address these challenges as well as compliance challenges by offering FedRAMP compliant environments to operate in.

What is Your Authorization Status?

AWS offers the following FedRAMP compliant services that have been granted authorizations, have addressed the FedRAMP security controls (based on NIST SP 800-53), used the required FedRAMP templates for the security packages posted in the secure FedRAMP Repository, has been assessed by an accredited independent third party assessor (3PAO) and maintains continuous monitoring requirements of FedRAMP:

AWS GovCloud (US), has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for high impact level. The services in scope of the AWS GovCloud (US) JAB P-ATO boundary at high baseline security categorization can be found within AWS Services in Scope by Compliance Program.

AWS US East-West (Northern Virginia, Ohio, Oregon, Northern California) has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate impact level. The services in scope of the AWS US East-West JAB P-ATO boundary at Moderate baseline security categorization can be found within AWS Services in Scope by Compliance Program.

What is Your FedRAMP Impact Level?

Customers can evaluate their high-impact workloads for suitability with AWS. Currently, customers can place their high-impact workloads on AWS GovCloud (US), which has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) for high impact level.

The authorization at DoD IL 6 allows DoD Mission Owners to process classified and mission-critical workloads for National Security Systems in the AWS Secret Region. The AWS Secret Region was built as part of the Commercial Cloud Services (C2S) contract and is available to the DoD on the AWS GSA IT70 schedule.

Company Description

AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon that includes a mixture of infrastructure as a service (IaaS), platform as a service (PaaS) and packaged software as a service (SaaS) offerings.

Contact Information and URL

https://aws.amazon.com/compliance/programs/

Google Cloud

What is Your Authorization Status?
Google Cloud supports FedRAMP High and FedRAMP Moderate compliance. See the full list of Google Cloud compliance offerings here.

What is Your FedRAMP Impact Level?
Google Cloud supports FedRAMP High and FedRAMP Moderate compliance. See the full list of Google Cloud compliance offerings here.

Company Description
Google is a trusted technology leader who understands how to help agencies transition from legacy architectures and utilize their data to fuel true mission success. Google Cloud provides cloud-native infrastructure with layered security, machine learning and analytics at web-scale to rapidly innovate and advance agency goals.
For more information: https://cloud.google.com/solutions/government/

Contact Information and URL
Google Cloud solutions for the federal Government: https://cloud.google.com/solutions/federal-government

Contact Google Cloud

Microsoft

Describe Your FedRAMP Solution
Microsoft Azure Government (authorized; high) is a government-community cloud that offers hyper-scale compute, storage, networking, and identity management services, with world-class security. A physically and network-isolated instance of Microsoft Azure, operated by screened U.S. citizens, Azure Government provides standards-compliant IaaS and PaaS that has now received a FedRAMP JAB P-ATO. All services are available immediately for supporting secure US government workloads, including CJIS, IRS 1075 FTI, HIPAA, DoD, and federal agency data.

Microsoft also offers Dynamics 365 for Government and Office 365 for Government as FedRAMP solutions.

What Challenges Does Your Solution Address?
Microsoft's government cloud services, including Azure Government, Dynamics 365 Government, and Office 365 U.S. Government meet the demanding requirements of the US Federal Risk and Authorization Management Program (FedRAMP), enabling U.S. federal agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud.

Microsoft government cloud services offer public sector customers a rich array of services compliant with FedRAMP, and robust guidance and implementation tools, including the FedRAMP High blueprint, which helps customers deploy a core set of policies for any Azure-deployed architecture that must implement FedRAMP High controls.

What is Your Authorization Status? Authorized

What is Your FedRAMP Impact Level? High

Company Description
Together with you, Microsoft Federal imagines the possibilities of what our government can do for people, organizations, the nation, and the world. We are unique among tech companies for the decades of trust we've earned in helping our federal customers achieve more. We combine mission understanding, deep engineering expertise, and breakthrough technology to empower a new era of Government.

Contact Information and URL
Victoria Sutch, Federal Channel Director, Microsoft, (703) 405-4323 fedchannelteam@microsoft.com

https://www.microsoft.com/en-us/federal/

ORACLE
Cloud

Describe Your FedRAMP Solution

Oracle Cloud is the first cloud designed to deliver better performance, manageability, security, and efficiency for any workload and application, so your agency can spend less time managing IT and more time innovating. Oracle offers a wide range of IaaS and PaaS services, as well as key industry partnerships, to solve every business need.

There are 6 main reasons why customers are choosing Oracle Cloud today:

1. Far easier to migrate enterprise-grade workloads and provide the expected level of performance and availability without significant modification.

2. Everything you need to develop cloud native applications. All of the innovations made in compute, security, and networking make cloud native applications perform better as well. Additionally Oracle cloud has the broad cloud services and partner ecosystem you need to build cloud native applications.

3. Autonomous services automatically secure, tune, and scale your workloads, reducing the risk and cost of human error. Choose from Autonomous Data Warehouse, Autonomous Transaction Processing, Autonomous JSON Database, Autonomous APEX, and Autonomous Linux.

4. Oracle Cloud provides the most support for hybrid cloud including a native VMware solution, Azure Interconnect, and numerous FastConnect partners.

5. Our approach to security – built-in, always on. We've designed security into the core experience of your application migration or build, and we've made most of our security tooling to be at no additional cost as part of your environment.

6. OCI offers superior price-performance. We offer consistent low service pricing around the globe. We also make it easier to work with Oracle by backing our services with the most comprehensive SLAs, not just for availability but also for the performance of our network and storage services and your availability to manage service through APIs at all times.

What Challenges Does Your Solution Address?

Oracle Cloud is a second-generation cloud built on security-first design principles and is the first public cloud built from the ground up to be a better cloud for every application. By rethinking core engineering and systems design for cloud computing, we created innovations that solve problems that customers have with existing public clouds, including cost.

What is Your Authorization Status?

Generally available services in the Oracle Gov Cloud are at FedRAMP High.

What is Your FedRAMP Impact Level?

Generally available services in the Oracle DOD Cloud are at DoD Impact Level 5

Company Description

Oracle offers a complete technology stack in the cloud, on premises, and in the data center. Our stack of products gives customers complete deployment flexibility and the unmatched benefits of application integration, powerful performance, high availability, scalability, advanced security, energy efficiency, and low total cost of ownership.

Contact Information and URL

https://www.oracle.com/industries/government/federal/

MultiCloud Solutions

Red Hat

Describe Your FedRAMP Solution
Red Hat OpenShift Service on AWS (ROSA) is a turnkey application platform that provides a fully managed Red Hat OpenShift service deployed and operated on AWS. Quickly build, deploy, and manage Kubernetes applications on the industry's most comprehensive application platform in AWS cloud.

With ROSA, you can use the wide range of AWS compute, database, analytics, machine learning, networking, mobile, and other services to build secure and scalable applications faster. ROSA comes with pay-as-you-go hourly and annual billing, a 99.95% SLA, and joint support from AWS and Red Hat. ROSA makes it easier for you to focus on deploying applications and accelerating innovation by moving the cluster lifecycle management to Red Hat and AWS. With ROSA, you can run containerized applications with your existing OpenShift workflows and reduce the complexity of management.

What Challenges Does Your Solution Address?
ROSA delivers the production-ready OpenShift that many enterprises already use on-premises today, simplifying the ability to shift workloads to the AWS public cloud as business needs change. OpenShift removes barriers to development and builds high-quality applications faster with self-service provisioning, automatic security enforcement, and consistent deployment. This helps customers accelerate change iterations with automated development pipelines, templates, and performance monitoring.

What is Your Authorization Status? In-Process

What is Your FedRAMP Impact Level?
Once approved, ROSA will have a FedRAMP High designation.

Company Description
The adoption of open principles helps the U.S. government start, accelerate and improve the art of digital transformation. As the world's leading provider of enterprise open source solutions, Red Hat uses a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container and Kubernetes technologies.

Contact Information and URL
https://www.carahsoft.com/redhat

703-871-8629

vmware®

Describe Your FedRAMP Solution
VMware Government Services (VGS) is a set of cloud service offerings designed to allow US government agencies and customers supporting the US government to move more sensitive workloads into the cloud.

What Challenges Does Your Solution Address?
A key offering of VGS is the VMware Cloud™ on AWS GovCloud (US) (VMC) IaaS. VMC brings VMware's rich Software-Defined Data Center software to the AWS GovCloud (US) Region and enables U.S public sector agencies and customers to securely run production applications across VMware vSphere®-based private, public and hybrid cloud environments, with optimized access to AWS services.

Jointly engineered by VMware and AWS, this on-demand service enables IT teams to seamlessly extend, migrate and manage their cloud-based resources with familiar VMware tools. VMC integrates VMware's flagship compute, storage and network virtualization products (i.e., VMware vSphere®, VMware vSAN™ and VMware NSX®) with VMware vCenter® management.

What is Your Authorization Status? JAB

What is Your FedRAMP Impact Level? High

Company Description
VMware Government Solutions provide the digital foundation for the evolution and transformation of government IT, enabling agencies to improve mission outcomes and meet constituent expectations for modern, efficient and cost effective services. VMware's interoperable cloud, app, networking, security and workspace solutions form a flexible digital foundation that enhances mission delivery, ensures continuity of operations and resiliency, and improves citizen and employee experiences while safeguarding data.

Contact Information and URL
fedramp-vmc@vmware.com

https://www.vmware.com/products/vmc-on-aws/govcloud.html

Cloud Service Providers

Describe Your FedRAMP Solution
Adobe Acrobat Sign for Government is a security-enhanced version of Adobe's industry-leading digital signature and document workflow solution, available to U.S. federal, state, local, and tribal governments as well as the contractors or commercial companies which support them. Capabilities include web forms, batch signing, automated workflows and document templates, as well as support for both citizen e-signatures and employee digital signatures.

What Challenges Does Your Solution Address?
Meeting the needs of constituents and communities increasingly means rethinking the way things have always been done. Agencies are responding to today's problems with creative approaches that improve workflows and deliver better digital experiences.

Adobe digital document solutions equip agencies to serve stakeholders with agility and imagination. We're proud to harness our history of creative and technological leadership in service of today's evolving government agencies.

What is Your Authorization Status?
Adobe Acrobat Sign for Government – is a SaaS Moderate FedRAMP Authorized product.

What is Your FedRAMP Impact Level?
Adobe Acrobat Sign for Government – is an IL2.

Company Description
Creativity is in our DNA. Our game-changing innovations are redefining the possibilities of digital experiences. We connect content and data and introduce new technologies that democratize creativity, shape the next generation of storytelling, and inspire entirely new categories of business.

Contact Information and URL
https://www.adobe.com/acrobat/contact.html

800-915-9430

Describe Your FedRAMP Solution

Cloud Security: Akamai extends security capabilities to Akamai's edge with cloud-based solutions that are designed to ensure the availability and security of your online properties. This includes our industry-leading DDoS mitigation, web application firewall, bot management, authoritative DNS, and threat intelligence.

Optimized Performance: Extending security capabilities and business logic to the edge has been shown to improve overall performance and public engagement. Akamai's edge can apply logic to adapt content to client users based on device capabilities, without needing to make additional callbacks. The offload not only reduces the operational impact on government resources, but also reduces operational costs.

Modernized Ecosystem: Collectively, the Akamai Intelligent Edge Platform and underlying solutions will empower you to have an agile MultiCloud environment with the foundational features for developing a SASE architecture. This includes providing TIC 3.0 security capabilities, a powerful suite of APIs for developers to integrate into a DevOps environment.

What Challenges Does Your Solution Address?

As agencies become fully entrenched in the new normal, Akamai's FedRAMP accreditation boundary ensures that you can continue to realize your mission for your constituents while staying secure, available, and compliant.

What is Your Authorization Status?

JAB PATO since 2013

What is Your FedRAMP Impact Level?

JAB Moderate

Company Description

Akamai powers and protects life online. Leading companies choose Akamai to build, deliver, and secure digital experiences. With the most distributed compute platform — cloud to edge — customers can build modern apps while keeping experiences closer to users and threats farther away. Learn about Akamai's security, compute, and delivery solutions at akamai.com.

Contact Information and URL

akamai@carahsoft.com
www.akamai.com

Describe Your FedRAMP Solution

AvePoint's Confidence platform powered by AvePoint Online Services for US Government is the industry's first and only 100% Microsoft Azure-based Software-as-a-Service (SaaS) platform for Microsoft 365. Requiring no installation or agents, this platform for US Government provides centralized management, governance, backup, reports, and ECM/records management for M365. It also provides backup for Dynamics 365, Salesforce, and Google Workspace.

What Challenges Does Your Solution Address?

AvePoint creates products that secure digital workplace collaboration. AvePoint supports this through a centralized management, governance, backup, reports, and ECM/records management for Microsoft 365.

What is Your Authorization Status?

Authorized

What is Your FedRAMP Impact Level?

Moderate

Company Description

Collaborate with confidence. AvePoint is the largest Microsoft 365 data management solutions provider, offering a full suite of FedRAMP-authorized SaaS solutions to migrate, manage and protect data. AvePoint Public Sector is an independent subsidiary of AvePoint. We serve more than 1,000 customers in 49 out of the 50 states, including 400 local governments and municipalities, every cabinet of the federal government, and all four branches of the DoD.

AvePoint Public Sector is headquartered in Arlington, Virginia. For more information visit https://www.avepoint.com/solutions/us-public-sector.

Contact Information and URL

Jay Leask, Director of Strategic Accounts and Solutions, Jay.Leask@avepoint.com
https://www.avepoint.com/solutions/us-public-sector

COPADO

Describe Your FedRAMP Solution

Copado GovCloud is a Salesforce-native DevSecOps Platform with a proven track record of accelerating Salesforce releases, bringing security and compliance into the end-to-end development pipeline and scaling across any number of production and sandbox instances.

Copado GovCloud is designed for both low-code and pro-code Salesforce developers and administrators. It makes it easy to release changes with automated version control for all major Git providers. Copado helps teams adopt modern DevOps practices that enable them to deliver more Salesforce features and value. Copado accelerates time-to-value for Salesforce applications, enhances developer efficiency, increases security visibility, improves Salesforce testing capabilities and enables digital cloud transformations.

Copado GovCloud helps federal agencies:

- Deploy Salesforce metadata to production and sandbox instances via automated Git integration for version control and branch management
- Execute change management (Including agile development processes, quality gates and code scanning)
- Prevent merge conflicts and overwrites through overlap awareness and conflict resolution
- Keep environments in sync and reduce sandbox refreshes through back-promotions
- Unlock continuous deployment and continuous integration (Including visual pipeline configuration)
- Enforce compliance rules for Salesforce metadata (Including rule creation, monitoring and enforcement of policies across user stories, Git snapshots and deployments)
- Seed test data across sandboxes to guarantee accurate quality assurance prior to production deployments.

What Challenges Does Your Solution Address?

The trends that forced the public sector to tackle digital transformation aren't going away — from rising customer demands to cyberattacks to the pandemic. As more agencies turn to low-code cloud platforms to address their digital needs, they often struggle to scale and accelerate their app development without compromising security and quality.

Copado GovCloud provides agencies with a user-friendly experience. This makes it easy for non-technical admins and business users to plan, build, verify, deploy and monitor development across clouds like Salesforce, Mulesoft, Heroku and Google. With built-in security and governance, Copado GovCloud enables agencies to respond faster, achieve higher levels of software quality, deliver more digital services and scale to unprecedented demands — all while reducing the need for pro-code experience.

Low-code DevOps platforms (like Copado GovCloud) help agencies realize the potential of their cloud platform and enable them to focus on building experiences that drive citizen trust and engagement.

What is Your Authorization Status?

FedRAMP "In Process"

What is Your FedRAMP Impact Level? Moderate

Company Description

Copado is the #1 DevOps & Testing Platform for Salesforce and the Cloud. Backed by Insight Partners, Salesforce Ventures and SoftBank Vision Fund, Copado leverages native CI/CD and Robotic Testing to drive digital transformation for 1,000+ of the most innovative brands on the planet — including the U.S. Department of Veterans Affairs, DC Health, California Department of Public Health and the Centers for Medicare & Medicaid Services. Copado handles over 50 million DevOps transactions per month and has a 100% rating on the Salesforce AppExchange.

Contact Information and URL

copado@carahsoft.com

https://www.copado.com/solutions/solutions-by-industry/public-sector/

CyberRes
A Micro Focus Line of Business

Describe Your FedRAMP Solution

CyberRes Fortify on Demand (FoD) is a cloud-based application security testing platform that enables customers to:

- **Start immediately, scale rapidly**
  FoD provides a fast and easy way to start an application security program with minimal upfront investment and the flexibility to scale with changing business needs. Additionally, there is no need to install, procure, and maintain hardware or hire and retain a large staff of application security experts.
- **Obtain fast results**
  With FoD, Agencies can expect accurate, detailed results, delivered on many assessments, all in minutes.
- **Access a centralized portal**
  User-friendly dashboards and reporting make it simple for Agencies to manage an application portfolio and collaborate across distributed teams. Furthermore, FoD allows Agencies to assess risk, initiate scans, analyze results, and remediate vulnerabilities based on prioritized recommendations.
- **Use industry leading security testing tools**
  FoD leverages industry leading static and dynamic application security testing (SAST and DAST) tools as recognized by independent analysts including Gartner. FoD also supports security testing of mobile applications (client and backend).
- **Access to CyberRes software security research**
  Agencies will have access to real-time threat intelligence updates from CyberRes Fortify security research.
- **Access to security experts**
  For assurance, all results are manually reviewed by application security experts. Customers can also rely on the support of a technical account manager to help manage the program.

What Challenges Does Your Solution Address?

- Identify and Eliminate Vulnerabilities Earlier Access Detailed Reporting of Static Scan Results and Vulnerability Management
- Conduct Dynamic Application Security Testing Flexible Plans to Fit Your Business' Mission

What is Your Authorization Status?

Currently FedRAMP authorized for CyberRes Fortify on Demand solution.

In process of obtaining additional authorizations for:

- Voltage File Analysis Suite
- ArcSight Intelligence
- NetIQ Identity Governance
- NetIQ Advanced Authentication

Company Description

CyberRes proud to partner with the US federal Government to bring the best Cyber Security Solutions to market. We have the expertise to help our customers navigate changing threat landscapes by building both cyber and business resiliency within their teams and organizations, and protect against the unauthorized exploitation of systems.

Contact Information and URL

Stan Wisseman – Chief Security Strategist
703-403-8549
stan.wisseman@microfocus.com

Site Contact Form: https://www.microfocus.com/en-us/cyberres/contact

CyberRes US Fed: https://www.microfocus.com/en-us/cyberres/industry/government-cyber-security

EQUIFAX

What is Your Authorization Status?
FedRAMP Ready

What is Your FedRAMP Impact Level? Moderate

Company Description
Equifax delivers data, analytics, technology, and expertise to transform knowledge into insights, empowering government agencies to make more informed decisions, maximize program efficiency, and improve the customer experience.

Equifax assists social service agencies throughout the benefit lifecycle, from initial determinations and renewals to monitoring life changes that impact ongoing eligibility.

Contact Information and URL
Jessica Giles, Equifax Manager, Carahsoft
jessica.giles@carahsoft.com, 703-871-8516

www.equifax.com/government

GENESYS

Describe Your FedRAMP Solution
Genesys Cloud CX is a composable all-in-one CX SaaS solution. This suite of cloud services for enterprise-grade communication, collaboration, and contact center management provides the ability to securely communicate with customers over a range of channels, including voice, text, and video conference. Genesys Cloud CX can also integrate seamlessly with customer call center systems to provide visibility into customer interactions with existing communication channels.

To provide additional functionality, Genesys Cloud CX allows customers to enable third-party integrations through AppFoundry, a Genesys marketplace of integrations supported by the Genesys Cloud CX application. Users of the application can also leverage self-service tools that provide speech-enabled Interactive Voice Response (IVR), voicebots, and chatbots, as well as tools to enhance workforce engagement management (WEM). These tools allow users to optimize Genesys Cloud CX for their unique requirements. A microservices-based architecture and API-first development supports rapid deployment and highly configurable components within the Genesys Cloud CX system.

The Engagement Platform delivers the utmost flexibility and control for your contact center experience. This solution leverages Genesys technology to provide the omnichannel functionality required for an optimized citizen engagement experience that enables citizens to communicate with your agency across all channels – including voice, email, SMS and web chat.

The Engagement Platform also provides key additional modular features such as workforce management, recording and quality management, analytics, AI and a robust reporting framework. The platform features a full range of secure capabilities to customize and operate contact centers of any size, supporting organizations' security, accessibility and privacy requirements. With the Engagement Platform, agencies can leverage a broad range of proven and certified implementation partners to guide and enable their contact center solution.

What Challenges Does Your Solution Address?
- Delivering seamless customer experiences that build pride and trust in government
- Eliminating data silos and optimizing the customer experience across the entire journey
- Freeing contact center staff from mundane and repetitive work so they can focus on the most complex issues
- Scaling government services quickly while delivering responsive and empathetic service at scale

What is Your Authorization Status?
- Genesys Cloud CX is an SaaS FedRAMP In Process solution
- The Genesys Engagement Platform is a PaaS FedRAMP Authorized solution

What is Your FedRAMP Impact Level?
- Genesys Cloud CX is FedRAMP In Process at the Moderate Impact Level
- Genesys Engagement Platform is FedRAMP Authorized at the Moderate Impact Level

Contact Information and URL
Genesys@Carahsoft.com

www.genesys.com

What is Your Authorization Status?
Informatica, an enterprise cloud data management leader, has achieved U.S. Government Federal Risk and Authorization Management Program (FedRAMP) Moderate Level designation under the sponsorship of the Department of State for the Informatica Intelligent Cloud Services (IICS) platform.

What is Your FedRAMP Impact Level?
Moderate Impact Level designation

Company Description
As the world's leader in Enterprise Cloud Data Management, we're prepared to help you intelligently lead—in any sector, category or niche. Informatica provides the foresight to become more agile, realize new growth opportunities or create new inventions. With 100% focus on data, we offer the versatility needed to succeed.

Contact Information and URL
For more information about Informatica Products and Services, please contact:
Informatica Solutions for Government
703-871-8622, Informatica@carahsoft.com

https://www.carahsoft.com/informatica#overview

Describe Your FedRAMP Solution
Bridge the gap between strategic goals and the day-to-day management of work. With increased visibility and alignment, you have the insights to support an outcome-driven approach to software development. Micro Focus Product and Portfolio Management (PPM) combines workflows and data to align investments with strategy. Top-down and bottom-up analytics power this strategic portfolio and project management tool. PPM provides critical information in real time to help you make the right investment decisions. It standardizes, manages, and captures the execution of project and operational activities as well as resources. Through continuous monitoring with smart KPIs, PPM takes advantage of what-if-scenarios to determine the right mix of deliverables versus investments.

What Challenges Does Your Solution Address?
Today's project management organization (PMO) struggles with time, cost, and resource management challenges, particularly visibility and data consolidation within the enterprise portfolio. Given these daily challenges, it is difficult for agency executives to see which projects and operational activities they should be working on to find out how much is left in their budget, to what capacity are resources being utilized, and how to align activities with mission demands.

What is Your Authorization Status?
SaaS offering currently in process. Existing PaaS, IaaS, and on-prem deployment options also available.

What is Your FedRAMP Impact Level? Moderate.

Company Description
Micro Focus is one of the world's largest enterprise software providers. We deliver mission-critical technology and supporting services that assist nearly every federal government agency manage core IT elements of their mission so they can run and transform—at the same time. With over 1800 patents issued and 900 pending, our extensive patent portfolio highlights Micro Focus' ingenuity and ever-evolving technology. We're committed to creating new and innovative solutions that help our government customers drive better mission outcomes.

Contact Information and URL
MicroFocus@carahsoft.com

PPM solution info | https://www.microfocus.com/en-us/products/ppm-it-project-portfolio-management/overview

MongoDB.

Describe Your FedRAMP Solution
MongoDB Atlas for Government is a separate environment of MongoDB Atlas, dedicated to meeting the demanding security and privacy needs of the US Government. It is a fully managed MongoDB service engineered and run by the same team that builds the database and MongoDB Atlas. It incorporates operational best practices we've learned from optimizing thousands of deployments across startups and the Fortune 100. Build on MongoDB Atlas for Government with confidence, knowing that you no longer need to worry about database management, setup and configuration, software patching, monitoring, backups, or operating a reliable, distributed database cluster.

What Challenges Does Your Solution Address?
The most innovative cloud database service on the market, providing the versatility needed to modernize legacy applications and support the unique requirements and missions of the US government – in a secure, fully-managed, FedRAMP environment.

What is Your Authorization Status? In-Process

What is Your FedRAMP Impact Level?
FedRAMP Moderate

Company Description
MongoDB is the next-generation data platform helping the Public Sector transform their mission critical challenges by harnessing the power of data. From local governments to federal agencies, MongoDB is used to create applications never before possible at a fraction of the cost and time of our competitors.

Contact Information and URL
MongoDB@carahsoft.com

https://www.mongodb.com/industries/government

New Relic.

Describe Your FedRAMP Solution
FedRAMP Moderate, Multi-Tenant, Hyper-Scalable SaaS Platform that includes AI, Telemetry Data Platform and Full Stack Observability.

What Challenges Does Your Solution Address?
Full Stack Observability with AI to Analyze, Understand and Troubleshoot system performance across an entire IT Estate, from applications and infrastructure to logs mobile applications, serverless applications, through to the end-user experience with one unified cloud platform to manage mission critical infrastructure -- increase uptime performance & reliability, meet SLA's, accelerate innovation and growth, reduce Op-EX and enhance customer experience.

What is Your Authorization Status?
38 Authorizations

What is Your FedRAMP Impact Level? Moderate

Company Description
Founded in 2008, New Relic is an ISV, Cloud Provider and leader in the Gartner Magic Quadrant for Application Performance Management. The New Relic One Cloud Platform offers Full Stack Observability with AI and a Telemetry Data Platform in one, unified SaaS solution to Government Agencies around the world.

Contact Information and URL
NewRelic@carahsoft.com

www.newrelic.com

okta

Describe Your FedRAMP Solution
The Okta Identity Cloud is the only FedRAMP Authorized, cloud-native identity and access management platform consistently named a leader by major analyst firms.

Okta's fully managed SaaS solution is delivered as a multi-tenant service built from the ground up. Customers benefit from weekly product updates, zero planned downtime, pre-built UIs, and well documented wizards / APIs that streamline time-to-value for customers. The result is maximum IT and end user productivity.

Our complete solution centralizes identity (and user behavior) across all your IT resources and Okta customers have the least amount of IT administration. We accomplish this by eliminating on-premises servers and the maintenance involved. This uniquely allows us to see the broadest set of data to deliver additional security controls to your environment.

What Challenges Does Your Solution Address?
Okta enables agencies to confidently modernize, adopt zero trust, and improve user experiences through secure identity management, multi-factor authentication with single sign-on, and least privilege access with continuous authorization.

What is Your Authorization Status?
Moderate Authorization, enabling federal customers to use the Okta service for unclassified workloads which includes DoD Impact Level 2

What is Your FedRAMP Impact Level?
Moderate, High (In Process)

Company Description
Okta is the leading independent provider of customer identity and access management. The Okta Identity Cloud is the only FedRAMP Authorized, cloud-native identity and access management platform consistently named a leader by major analyst firms. Already trusted by 14,000+ customers, Okta enables government agencies to confidently modernize and adopt zero trust through secure identity management, multi-factor authentication with single sign-on, and least privilege access with continuous authorization. And with more than 7,000 pre-built, validated integrations with both cloud and on-premises systems, Okta makes deployment simple, reliable, and scalable.

Contact Information and URL
federal@okta.com

okta.com/publicsector

SailPoint

Describe Your FedRAMP Solution
SailPoint's Identity Security is a multi-tenant SaaS platform that gives organizations a complete view into the security of their enterprise by delivering timely, optimal access to their identities. Identity Security SaaS will consist of SailPoint's IdentityNow, Cloud Access Management, and AI-Driven Identity offerings.

SailPoint Identity Security combines identity data with the power of AI and machine learning to drive stronger security and compliance across your entire organization. Because if you don't have a way to analyze your identity data, you're missing a key tool that can help you become proactive and make better access decisions.

SailPoint provides a fully automated approach to provisioning access based on policies you set. Give IT teams complete visibility to monitor and manage all access in real time.

SailPoint simplifies and streamlines the complexity of compliance management through a unified identity security framework.

Our identity security platform makes it easy to turn large amounts of identity data into actionable insights. From user attributes and roles to access history and entitlements as well as the identification of identity outliers, our access insights provide rich intelligence to transform your identity security program into an essential strategic resource.

SailPoint Cloud Access Management allows you to get complete visibility and control across your cloud infrastructure and workloads, detect potential anomalies, and better enforce access policies across all users. >

What Challenges Does Your Solution Address?

- Maximize Day 1 productivity with automated provisioning of access to apps and data
- Automatically adjust access as users change roles, take on new projects or leave the organization
- Provide users with self-service access requests and automated actions built from identity-based policies
- Equip business managers with AI-driven recommendations that indicate when it's safe to grant access
- Ensure access is always right sized and in compliance for each user
- Speed up and improve the accuracy of access certifications with automated recommendations that focus on areas of highest risk
- Enforce Separation of Duties (SoD) policies across millions of points of access and flag violations instantly
- Centrally manage and dynamically update access policies across the organization
- Complete auditing and reporting requirements in record time and with confidence
- Discover identity access outliers with AI-driven visibility into access privilege
- Identify potential risks, such as abnormal entitlements and dormant or orphaned accounts
- Determine what access users should have versus what access they currently have
- Receive recommended remediation steps that integrate into certification campaigns
- Review dashboards and reports to track the effectiveness of your identity program
- Find and manage high-risk access using policies that continuously search access to identify risks
- Simplify access visibility with an interactive graphical map of access, from identities to entitlements to resources
- Identify excess privileges and "right-size" access by finding unused sensitive entitlements across the MultiCloud environment.

What is Your Authorization Status? In-process

What is Your FedRAMP Impact Level? Moderate

Company Description
SailPoint is the leader in identity security for the cloud enterprise. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, ensuring workers have the right access to do their job – no more, no less.

Contact Information and URL
SailPoint@carahsoft.com

https://www.sailpoint.com/identity-for/government/

Describe Your FedRAMP Solution
Salesforce Government Cloud Plus is a partitioned instance of Salesforce's industry-leading Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), multi-tenant community cloud infrastructure specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs).

Government Cloud Plus gives customers a compliant and secure environment to deploy Salesforce's Customer 360 CRM and its industry solutions.

What Challenges Does Your Solution Address?
Many government agencies today rely on outdated systems with limited ability to upgrade and adapt to the needs of modern government. The result is

costly infrastructure, dated processes, complicated workflows, an overburdened workforce and poor service delivery for citizens. In addition, as governments deal with diverse and rapidly changing national and global events, they need to maintain continuity of operations, adapt to a remote workforce and deliver new services in times of need. To do this, government agencies of all types and sizes need access to a complete technology platform in order to deliver needed services, scale to unprecedented demands and connect to citizens on their channel of choice.

Salesforce delivers the agility, speed and scale that federal, state, and local governments, as well as government contractors, need to address employee and citizen needs while lowering IT cost and complexity. This includes access to customer relationship management, service, platform, integration, and analytics solutions, to help government customers and contractors achieve mission success and digital transformation across use cases such as workforce management and development, health and social services, case management, grants management, licensing, permitting, and inspections and much more.

What is Your Authorization Status?
Salesforce Government Cloud Plus has achieved a FedRAMP Provisional Authority to Operate (P-ATO) at the High Security Impact Level.

What is Your FedRAMP Impact Level? High

Company Description
Salesforce helps bring the public sector and customers together. Salesforce Customer 360 for Public Sector is an integrated platform for public services that brings mission-critical capabilities to life - enabling relationship management, case management, team collaboration, integration, and insights. For more information, visit www.salesforce.com/government.

Contact Information and URL
salesforce@carahsoft.com

salesforce.com/government

SAP NS2 NATIONAL SECURITY SERVICES

Describe Your FedRAMP Solution
NS2 Secure Cloud provides a secure, connected, and flexible platform that arms government and regulated industries against increased threats and cyberattacks by protecting their critical data in the cloud. Organizations face new challenges every day which is where the sovereign cloud comes in with a DoD IL4 allowing agencies the assurance that they are meeting to the utmost security and compliance requirements.

What Challenges Does Your Solution Address?
It aims to reduce dependence on multinational cloud providers and, in accordance with local laws and customs, ensure the cloud services are provided in a secure and transparent manner.

What is Your Authorization Status?
FedRAMP Authorized // Moderate

What is Your FedRAMP Impact Level? IL4

Company Description
We are SAP NS2. Or NS2 for short. At NS2 we deliver security for SAP enterprise products all over the globe. We also innovate and develop secure products that support your mission. Security is our middle name and it's in everything we do.

Contact Information and URL
Sapns2@carahsoft.com

https://www.sapns2.com/

splunk>

Describe Your FedRAMP Solution
Splunk Cloud™ has received FedRAMP authorization at a moderate impact level. Achieving FedRAMP authorization from the General Services Administration (GSA) FedRAMP Program Management Office (PMO) brings the power of Splunk Cloud to agencies that are eager to remove

the barrier between data and action and turn data into doing. As a result, federal agencies and their partners will now be able to leverage the assurance of the FedRAMP program to solve their toughest IT, security and IoT challenges with Splunk's Data-to-Everything Platform.

What Challenges Does Your Solution Address?

We are living in a time of unprecedented change, driven by an explosion of new technologies and new innovations. This change has created a never-ending flow of data from countless sources, however, the value of data remains trapped for most federal agencies. Splunk Cloud enables agencies to remove the barriers between data and action, allowing them to make confident decisions and take decisive action on data to help achieve mission success.

What is Your Authorization Status?

Thousands of public sector organizations worldwide are leveraging the Splunk Data-to-Everything platform, including all three branches of the U.S. government and 15 cabinet-level departments. For more information on Splunk and Splunk Cloud with FedRAMP visit the Splunk website. For additional information related to the Splunk FedRAMP package, please visit the FedRAMP PMO Marketplace.

What is Your FedRAMP Impact Level?

FedRAMP Moderate, Impact Level 5

Company Description

The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative.

Contact Information and URL

https://www.splunk.com/en_us/products/splunk-cloud-platform.html?301=/en_us/software/splunk-cloud.html

Contact Sales | https://www.splunk.com/en_us/talk-to-sales.html?expertCode=sales

TANIUM

Describe Your FedRAMP Solution

Tanium Cloud for US Government (TC-USG) is a Converged Endpoint Management Platform that is pre-configured out-of-the-box, fully managed by Tanium, and FedRAMP Ready at the Moderate-Impact level.

The solution gives federal organizations full visibility into their IT environment, the control to take comprehensive action and a single source of truth for all endpoint data, at scale.

With TC-USG, organizations can combine their security and operations functions into one console which allows siloed teams to work from the same endpoint data set – making it easier to find vulnerabilities across the organization and take action quickly. And, because Tanium manages the software as a service, federal IT teams don't have to allocate additional resources to manage the solution. Software releases, patches and general maintenance are all handled by Tanium, which means teams can focus precious time on higher value activities like threat hunting or security data analytics.

What Challenges Does Your Solution Address?

The more physical infrastructure the government supports, the more difficult it is to inventory and secure. A large portion of all federal endpoints are more off-campus now than ever - creating the need for a greater focus on threat hunting, and security data analysis, using real-time data. But with a workforce still largely tasked with managing legacy, on-premises tools, federal IT teams are too busy pushing software updates manually, replacing and maintaining old servers, and supporting on-premises tools, to respond to modern threats as proactively as they'd like. With more and more infrastructure to manage, each legacy asset represents a threat vector, which leaves federal organizations vulnerable.

Organizations lack:

- Visibility into unmanaged, offline or off-VPN assets
- Control across all endpoints, which creates a lack of certainty around things like patch status, software license usage and out of date compliance policies
- A single source of truth for endpoint data, when multiple point tools are used to manage IT security and operations

What federal government entities need is the ability to manage all their endpoints, on, or off-network from a single cloud-based platform that can reduce risk by retiring servers and outdated hardware, shift staff focus to higher value activities and get certainty with real-time visibility into their IT environment - at scale.

What is Your Authorization Status?
Tanium is a FedRAMP Ready Cloud Service Offering, at the Moderate-Impact level.

What is Your FedRAMP Impact Level? Moderate.

Company Description
Tanium is the platform that over half the Fortune 100, numerous government organizations and the U.S. Armed Forces trust to gain visibility and control across all endpoints. Our approach gives IT operations, security and risk teams confidence to manage, secure and protect their networks at scale. See and control every endpoint, everywhere. That's power of certainty.

Contact Information and URL
tanium@carahsoft.com

https://www.tanium.com/solutions/federal-government/

Describe Your FedRAMP Solution
Tenable.io FedRAMP is a risk-based vulnerability management platform that gives you visibility into your entire attack surface so that you can identify, investigate and prioritize vulnerabilities. Tenable.io provides the industry's most comprehensive vulnerability coverage with the ability to predict which security issues to remediate first. Using a diverse array of sensors to continuously gather and analyze security and vulnerability data, agencies get a real-time, continuous view of all assets- both known and previously unknown. Centrally managed and self-updating, Tenable.io leverages Nessus sensors, a mix of active scanners, lightweight agents and passive network monitoring to maximize scan coverage. Tenable.io's web-based UI provides agencies with a complete view of their attack surface and security and compliance posture.

Tenable.io Web Application Security (WAS) delivers safe and automated vulnerability scanning of web applications. Integrated with Tenable.io FedRAMP,agencies can view vulnerable web app components and custom code vulnerabilities alongside agency IT and cloud assets and use risk scores to identify vulnerabilities with the highest business risk.

What Challenges Does Your Solution Address?
As federal agencies focus on modernizing their IT infrastructure, Tenable.io and WAS provide a unified solution to deliver continuous visibility, critical context and actionable insight to protect complex networks and sensitive information, while adhering to compliance standards and regulations. We provide the security necessary for federal customers to move their workloads to the cloud and ensure they are compliant across cloud platforms. By combining vulnerability data, threat intelligence and data science, Tenable FedRAMP authorized solutions allow agency security leadership to understand their risk and quickly determine which vulnerabilities to fix first.

What is Your Authorization Status? Authorized

What is Your FedRAMP Impact Level? Moderate

Company Description
Tenable® is the Cyber Exposure company. Over 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform.

Contact Information and URL
tenable@carahsoft.com

https://www.tenable.com/solutions/government/us-fed

Please visit our sponsor resource hub pages by clicking here!

HyperScaler Cloud Providers

aws Google Cloud Microsoft ORACLE Cloud

MultiCloud Solutions

Red Hat vmware

Cloud Service Providers

Adobe Akamai AvePoint COPADO

CyberRes A Micro Focus Line of Business EQUIFAX GENESYS Informatica

MICRO FOCUS Government Solutions MongoDB New Relic okta

SailPoint salesforce SAP NS2 NATIONAL SECURITY SERVICES splunk>

TANIUM tenable

Scan Here

To learn more about what FedRAMP solution is right for you.

GOVFORWARD®

MultiCloud Series Event

SAVE THE DATE

For the fourth consecutive year, Carahsoft is bringing together leaders from federal and state government and the IT industry to discuss the evolution of FedRAMP and cloud security policies, marketplace technology advances and success stories.

FCW | FedRAMP Summit

7:30am-3:30pm Wednesday, August 24, 2022
JW Marriott, Washington DC and Online

As the FedRAMP program approaches the end of its first decade, an increased threat landscape has prompted changes throughout government.

Join FCW, Carahsoft and executives from government and industry for our second 2022 Summit on FedRAMP. During this hybrid event, we'll explore the new policy developments, learn how the changing threat environment is challenging agencies, and hear lessons learned from the log4j vulnerability.

Through government keynotes, panel discussions, master classes and networking, attendees will come away with a better understanding of:

- What the proposed rules on incident reporting can mean for agencies
- How a threat-based approach to risk management offers more security
- How new data on threats and responses is helping create new frameworks
- How state and local governments are progressing with StateRAMP
- …and more

Register Today and Learn More at govforward.com!
This site also features all the resources and on-demand presentations from the May 12, 2022 GovForward Policy Headliner Summit.

For more information, visit Carahsoft.com/FedRAMP
or contact us at govforward@carahsoft.com

carahsoft® The Trusted Government IT Solutions Provider®