carahsoft The Trusted Government IT Solutions Provider®

FedRAMP Buyer's Guide for Government

Empowering Federal Agencies: A Comprehensive Guide to Efficiently Adopting Cloud Solutions with FedRAMP

FEATURING: ***Impact Levels*** • ***Marketplace Breakdown*** ***Program Growth*** • ***Policies & Executive Orders*** ***Our FedRAMP Portfolio*** • ***Contract Vehicles***

powered by GovExec

carahsoft.

Thank You for Attending!

GOVFORWARD®

The ATO and Cloud Security Summit

July 24, 2025 | 8:00am

Waldorf Astoria,
Washington, D.C.

Scan the QR to explore
Carahsoft's FedRAMP Solutions
and view additional resources

Table of Contents:

4
Program Introduction

7
Key Players in the Authorization Process

8
Rev. 5 Agency Authorization Process

10
The Future of FedRAMP: Understanding FedRAMP 20X

12
Impact Levels

13
Marketplace Breakdown

14
Program Growth

16
Success Stories

34
FedRAMP Portfolio

52
Contract Vehicles

Welcome to the FedRAMP Buyer's Guide for Government!

FedRAMP enables Federal agencies to adopt secure cloud solutions efficiently and confidently through its streamlined approach to security assessment, authorization, and continuous monitoring for cloud service offerings. For government agencies, the implementation of FedRAMP is essential to maintaining high standards of security and compliance while transitioning to cloud services.

Carahsoft represents a wide array of FedRAMP offerings and supports the procurement and deployment of government-focused solutions to help agency partners meet their mission needs.

With today's current environment of Rev. 5, our government customers have leveraged thousands of reuse authorizations across hundreds of FedRAMP-authorized cloud services that we support. With such a substantial record of reuses, FedRAMP stands out as one of the most cost-effective, time-efficient, and security-enhancing programs in the history of government IT.

In this guide, we delve into the FedRAMP program, exploring its benefits, policies, and pathways to authorization. We also share case studies and best practices to help Federal agencies maximize the potential of FedRAMP solutions, ensuring fast and secure deployment to meet mission needs.

Program Introduction

FedRAMP Overview

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud service offerings (CSOs). Designed to be a cost-effective and risk-based approach to Federal CSO adoption, the program is built on the NIST Special Publication 800-53 framework. This common security framework and standardized baseline allows agencies to reuse authorizations, thereby eliminating duplicative efforts and reducing overall costs.

Mandatory Authorization

FedRAMP authorization is mandatory for all Cloud Service Offerings (CSOs) used by executive agencies, making it essential for Cloud Service Providers (CSPs) to ensure their solutions meet these rigorous security standards. Codified into law through the FedRAMP Authorization Act – signed in December 2022 as part of the FY23 National Defense Authorization Act (NDAA) – this legislation formally codifies the program, which previously existed only under a 2011 OMB memorandum, establishing it in statute with formal congressional oversight.

The Act introduces a presumption of adequacy, meaning cloud solutions that have achieved FedRAMP authorization are presumed secure and eligible for reuse across Federal agencies unless there is a demonstrable need for additional security requirements. It also establishes the Federal Secure Cloud Advisory Committee (FSCAC) to foster stronger communication between the Federal government and industry. The FSCAC includes 15 members, five of whom represent CSPs.

"There is established within the General Services Administration the Federal Risk and Authorization Management Program. The Administrator, subject to section 3614, shall establish a Government-wide program that provides a standardized, reuseable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies."

FY23 National Defense Authorization Act (NDAA)

FedRAMP Scope

The 2024 OMB FedRAMP memo M-24-15 defines what products are in-scope / out-of-scope for FedRAMP.

Scope Category	In-Scope	Out of Scope
Cloud Computing and Services	IaaS, PaaS, and SaaS that create, collect, process, store, or maintain Federal information on behalf of a Federal agency	Information systems used only for a single agency's operations, hosted on cloud infrastructure or platform, and not offered as a shared service or do not operate with a shared responsibility model
Social Media and Communication Platforms	Not Applicable	Social media and communications platforms used in accordance with agency social media policies
Search Engines	Not Applicable	Search Engines
Commercially Available Information Services	Cloud services that collect Federal information	Widely available services that provide commercially available information to agencies but do not collect Federal information
Ancillary Services	Cloud services critical to Federal operations	Ancillary services whose compromise poses a negligible risk to Federal information or information systems, such as systems that make external measurements or only ingest information from other publicly available services
Other Categories	Determined by FedRAMP Director with OMB approval	Any other categories of products or services identified for exclusion by the FedRAMP Board, with the concurrence of the Federal CIO

Clarifying FedRAMP Scope: RFC-0010

To support consistent application of FedRAMP scope exclusions defined in OMB M-24-15, the PMO issued RFC-0010: Scope Interpretation Technical Assistance. This draft guidance provides agencies with detailed examples and decision-making criteria to determine when cloud services fall outside of FedRAMP's applicability. It reinforces that applicability depends on how the agency uses the service – not just on the type of service – and emphasizes that exclusions must be assessed on a case-by-case basis.

Key Players in the Authorization Process

Successfully navigating the FedRAMP authorization process requires a clear understanding of the key stakeholders involved. Each organization plays a distinct role in evaluating, approving, and maintaining secure cloud offerings for Federal use. The table below outlines each participant's responsibilities:

Stakeholder	Role
Agencies	• Partner with CSPs to authorize cloud solutions • Procure FedRAMP Authorized cloud solutions • Oversee Continuous Monitoring for each authorized system in use
General Services Administration	• Resources, administers, and operates the FedRAMP PMO, and is responsible for the successful implementation of FedRAMP. • Responsible for defining core security expectations. • Develops best practices and contract clauses for cloud procurement.
FedRAMP Board	• Primary decision-making body. • Define/update FedRAMP requirements. • Monitor agency authorization processes.
Cloud Service Providers (CSPs)	• Navigate various pathways to FedRAMP authorization. • Conduct Continuous monitoring.
Third Party Assessment Organizations (3PAOs)	• Perform initial and periodic assessments of cloud systems to ensure they meet FedRAMP requirements.
FedRAMP Enablement Partners	• Advisory/accelerator partners help expedite the timeline required for a CSP to achieve FedRAMP Authorization.

Rev. 5 Agency Authorization Process

The Agency Authorization pathway remains the primary and most widely used method for CSPs to achieve FedRAMP authorization. In this approach, a Federal agency partners with a CSP to review and approve a cloud service offering based on the FedRAMP Rev. 5 security baseline.

The FedRAMP authorization process for agencies involves three key phases:

1 Preparation

- An optional Readiness Assessment and obtaining the "FedRAMP Ready" designation
- The CSP formalizes a partnership with an agency sponsor*

2 Authorization

- A Third Party Assessment Organization (3PAO) conducts a full security assessment, including the Security Assessment Plan (SAP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M)
- The agency reviews the security documentation and issues an Agency Authority to Operate (ATO)
- The FedRAMP Program Management Office (PMO) performs a final review and designates the CSO as FedRAMP authorized.

3 Continuous Monitoring

- CSPs are required to provide periodic security deliverables to all agency customers on a monthly and annual basis.

**The FedRAMP PMO does not formally recognize the concept of an "agency sponsor" because the ATO granted by the initial authorizing agency is not a government-wide risk acceptance, but rather an acceptance of the risk on behalf of the initial authorizing agency. The term "sponsor" is widely used however, especially among industry stakeholders.*

Initial Authorizing Agency Responsibilities

The initial agency partner plays a crucial role in supporting and guiding a CSP through the FedRAMP authorization process. This includes providing guidance on security controls, conducting risk assessments, overseeing continuous monitoring, and granting an ATO.

The quality of the authorization package significantly impacts the agency level of effort required. As the first government entity to review the security documentation, the initial agency must address any necessary remediations, which can be time-consuming. To mitigate these challenges, Carahsoft connects CSP partners with advisory and accelerator experts who have a track record of success. This collaboration helps produce high-quality packages with a reduced risk of remediation, thereby de-risking the investment for agencies considering an initial partnership.

The initial agency partner is not responsible for continuous monitoring oversight on behalf of agencies that reuse the FedRAMP ATO. Each subsequent agency that issues a reuse ATO for a cloud solution must review the CSPs continuous monitoring activities to ensure a sufficient security posture for its own use.

The Future of FedRAMP: Understanding FedRAMP 20X

Announced in March 2025, FedRAMP 20X is a new initiative aimed at modernizing the authorization process by emphasizing automation, reducing documentation, and removing unnecessary delays. The proposed future model would allow CSPs to submit directly to FedRAMP, bypassing the need for a sponsor, and leverage automated technical validations in place of narrative explanations and manual reviews. However, it is important to note that these changes are in early stages of development, and timelines for full implementation remain uncertain.

The first pilot phase of FedRAMP 20X is now open to public participation for cloud-native SaaS products at the FedRAMP Low impact level. Future phases are expected to include Moderate and High baselines, as well as multi-service and infrastructure offerings. As part of the Phase One pilot, CSPs can submit machine-readable files with validation evidence tied to new Key Security Indicators (KSIs) developed for FedRAMP Low. Submissions are reviewed by a 3PAO and the PMO, and successful CSOs receive a 12-month authorization and a prioritized path to FedRAMP Moderate. Unlike the traditional process, this pathway does not require agency sponsorship.

To support these changes, the PMO has launched several working groups focused on key modernization areas including continuous monitoring, automation, and the integration of existing commercial frameworks. It has also issued Requests for Comment (RFCs) on changes to the boundary policy, 3PAO requirements, and a proposed update to the significant change process. This collaborative approach highlights a broader shift: the PMO is moving from direct oversight to setting the guardrails for scalable and risk-based compliance.

The PMO has already begun operationalizing parts of the 20X initiative. In April 2025, the PMO authorized 29 CSOs – bringing the year-to-date total to 73 – and reduced the final review queue to just 25 packages, the lowest level since July 2022.

Process Comparison	Pre-March 24th Legacy Agency Authorization Process	Short Term Post March 24th Rev. 5 Agency Authorizations Continue	Proposed Long Term Post March 24th FedRAMP 20X
Current Applicability	**Fully enforced** FedRAMP required for use of cloud services handling federal information	**Still fully enforced** Vendors must comply with Rev. 5 to pursue federal opportunities	**Proposed framework is in early stages** Currently applicable only to a limited set of cloud-native SaaS offerings at FedRAMP Low, with broader applicability and timelines still to be determined
Sponsorship Requirement	**Required** CSPs needed an agency sponsor to begin authorization process	**Required** continues as before with no immediate changes	**Not required** CSPs submit directly to FedRAMP, bypassing the need tfor a sponsor
Review Process	PMO "triple check" reviews were standard, involving thorough manual oversight and leading to a review backlog	PMO phasing out "triple check" reviews; agencies now finalize security reviews	Automated validations replace manual reviews, speeding up the process
Impact Levels	Low, Moderate, and High available	Low, Moderate, and High available under Rev. 5	Phase One pilot open to public for cloud-native SaaS CSOs at FedRAMP Low; Moderate and High in future phases
Documentation Requirements	Detailed narrative documentation required to explain security controls	Continues with existing requirements; no immediate reduction in documentation	Greatly reduced; focus shifts to automated validations and key security layers
Role of PMO	Central to the authorization and monitoring process, providing guidance and oversight	PMO adjusting its role, focusing on clearing existing backlogs and reducing direct reviews	Sets standards and frameworks, shifting more responsibility to agencies and industry
Cost to CSPs	Can be high due to comprehensive documentation and thorough review processes	No immediate change, CSPs continue to bear high costs	Potentially lower costs due to reduced documentation and faster validation, though investment and innovation in validation tools will be required
Timeline for authorization	Longest; ~9 month review backlog at the PMO	Faster as PMO backlog is cleared, but still reliant on manual processes	Potential to be significantly faster with automation, goal is authorization in a matter of weeks
Security Standards	Uniform standards enforced centrally by the PMO	Standards remain uniform, but agency AO's have final say, which may introduce some variability	Standards set by the PMO, but implementation and compliance are industry-driven
Role of 3PAO	Integral to the review process, providing third party verification of security controls	Continues to provide critical validation of security controls before agency review	Uncertain; the role of 3PAOs may evolve, potentially reducing in scope as validations become more automated.

Impact Levels

FedRAMP categorizes CSOs into different impact levels based on the potential adverse effects on an agency's operations, assets, or individuals:

Impact Level	Security Controls (Rev. 5)
Low Suitable for CSOs where the loss of confidentiality, integrity, and availability would result in limited adverse effects.	156
Low Impact SaaS (LI-SaaS) Reserved for SaaS applications that do not store Personal Identifiable Information (PII) beyond basic login information. Consolidated security documentation requirements and fewer security controls needing testing and verification compared to a standard Low Baseline authorization.	156
Moderate Suitable for CSOs where the loss of confidentiality, integrity, and availability would result in serious adverse effects.	323
High Applicable to high-impact data systems, such as law enforcement, financial, and health systems, where loss could result in severe or catastrophic adverse effects.	410

Marketplace Breakdown

The FedRAMP Marketplace categorizes CSOs into three categories:

Ready

The CSP/3PAO has completed the Readiness Assessment Report (RAR) and received approval from the FedRAMP PMO. Can be completed without an agency sponsorship.

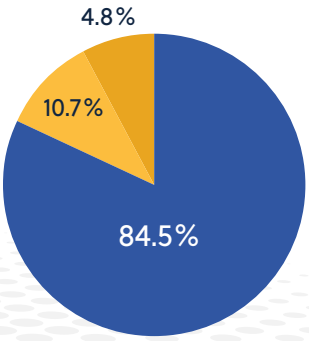
In Process

The CSP is actively working towards FedRAMP authorization, and the security documentation is currently being vetted through the ATO process by either the agency sponsor or FedRAMP PMO.

Authorized

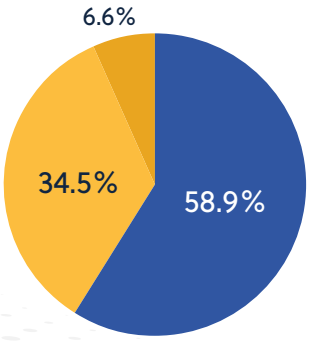
The CSO has successfully completed the FedRAMP Authorization process and the FedRAMP PMO has signed a FedRAMP ATO. This designation indicates that the FedRAMP compliance requirements have been met and the security package is available for agency reuse.

The following series of charts provide a detailed breakdown of key CSO statistics from the FedRAMP Marketplace, accurate as of July 2025:



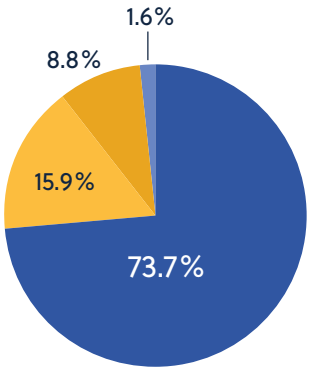
CSO by Service Model Type

- SaaS
- PaaS
- IaaS



CSO by Deployment Model

- Gov. Community Cloud
- Public
- Hybrid



CSO by Impact Level

- Moderate
- High
- LI-SaaS
- Low

Program Started

100

Authorized CSOs

2011

2014

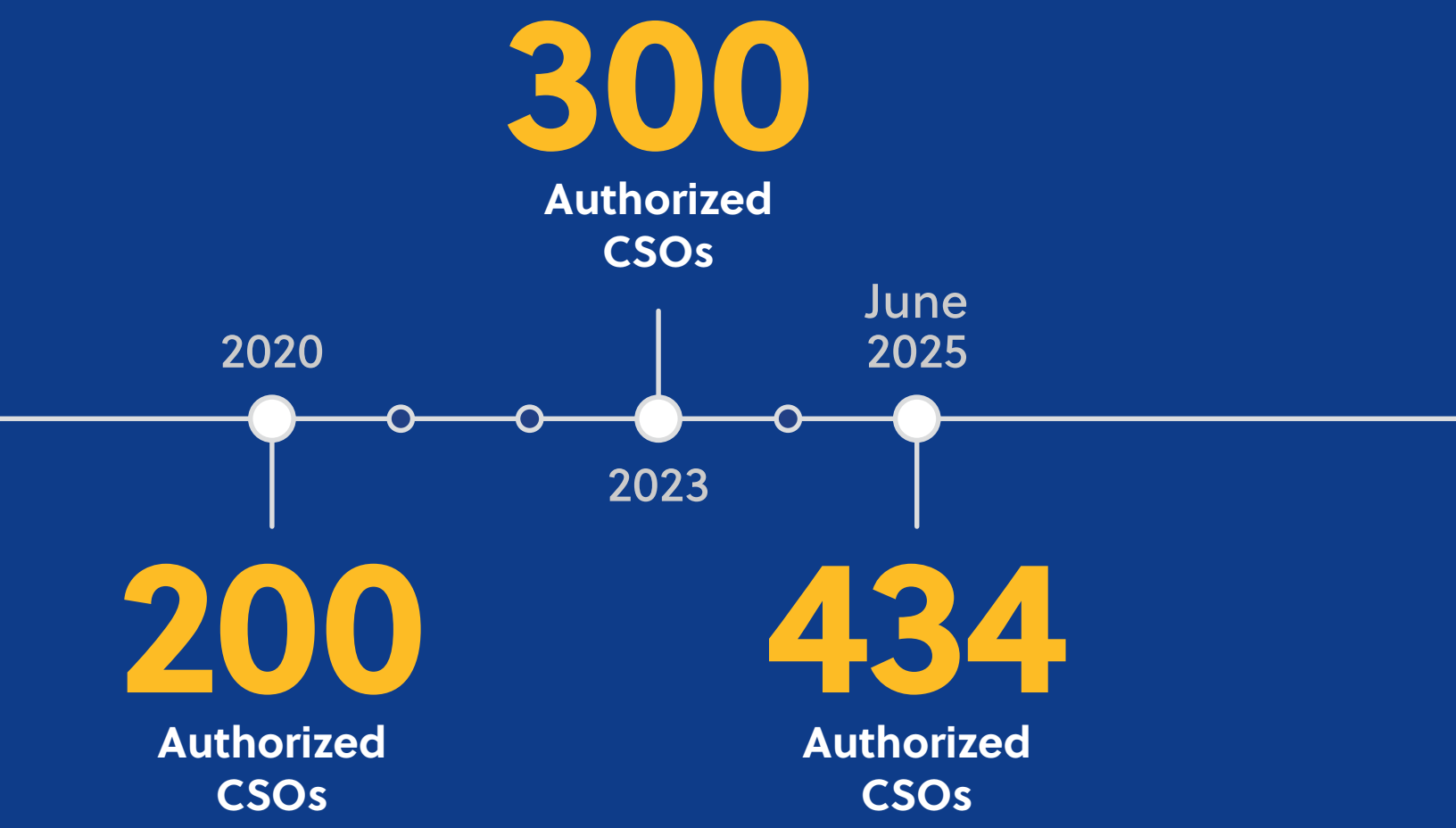
2018

20

Authorized CSOs

Program Growth

FedRAMP continues to be a major catalyst for secure cloud adoption across the Federal government. The program's emphasis on reuse allows agencies to adopt authorized cloud solutions more efficiently, saving time and resources by eliminating duplicative security assessments. The FedRAMP Authorization Act further reinforces this by establishing a "presumption of adequacy," meaning once a service is authorized by one agency, it is presumed secure for use by others. This streamlined approach supports the government's growing investment in cloud technologies and its ongoing efforts to strengthen cybersecurity.



FedRAMP is here to stay, and it's only growing, with FedRAMP 20x on the horizon, the time and cost to market for cloud solutions should only continue to decrease. The program will not only keep the same pace, but it will be scaled to protect our nation's systems.

Success Stories

Federal agencies are accelerating their cloud adoption and strengthening security by leveraging FedRAMP-authorized solutions from Carahsoft's trusted technology partners. Discover how agencies like yours are meeting mission demands while maintaining compliance through proven cloud innovations.

Browse Success Stories from our 2024 Edition:

eGain:
Knowledge-Powered Digital Journey to Improve Citizen Experiences Across Touchpoints

OnSolve:
5 Ways OnSolve Helps Federal Agencies Strengthen Resilience

Wolters Kluwer:
Reducing Administrative Overhead With Authorized Cloud-Based Tools

MongoDB.

Migrating to Compliant Cloud Solutions

Utah is one of the fastest-growing states in the United States. Between 2010 and 2020, the Utah population increased by 18.4% (compared with a national average of 7.4%). As it grows, the state is leveraging technology to provide better services to people.

The Challenge:

Utah's Electronic Resource and Eligibility Product (eREP) software helps caseworkers determine people's eligibility for benefits programs. Caseworkers access eREP for more than 60 social services, including food stamps, Medicaid, and childcare assistance. The application itself stores electronic case files and uses that information and a rules engine to calculate benefits.

The state's Department of Technology Services had been using MongoDB Atlas as eREP's primary database since 2016. MongoDB Atlas worked well for the state's use case because it stores files using BSON, which allows for efficient storage and compression. This significantly lowers storage volumes — and thus costs — for the department's databases. MongoDB Atlas can also store and retrieve large documents quickly — a crucial benefit given Utah's higher-than-average family sizes, which can make individual case files up to 16 MB. In 2022, the department had around 15 MongoDB nodes and wanted to upgrade to a fully managed version of MongoDB Atlas as part of its cloud transformation.

"The biggest chunk of the eREP application is in MongoDB Atlas. MongoDB was a very suitable product for us to store all the documents that we create. We tried some other solutions, but they could not match MongoDB."

Manoj Gangwar
Principal Data Architect,
Department of Technology Services at State of Utah

In that same year, the governor of Utah mandated that the state migrate its IT solutions to the cloud to better serve Utah's citizens. eREP had previously been hosted in a physical data center, so the state began migrating eREP to Amazon Web Services (AWS) in response to the new directive.

The Department of Technology Services had two primary requirements for the migration. First, as a government agency, it needed to use cloud technology that met the standards of the Federal Risk and Authorization Management Program (FedRAMP), a federal compliance program that evaluates cloud services for security. Second, because the solution was so critical for caseworkers, the department wanted a backend database that could handle large documents and deliver results quickly.

The Solution:

In 2022, the Department of Technology Services migrated eREP to MongoDB Atlas for Government. MongoDB Atlas for Government is a secure, fully managed, FedRAMP Moderate-authorized product for United States government agencies to deploy, run, and scale MongoDB databases in the cloud. It provides the high-security standards that the State of Utah needs to comply with as well as eREP's required level of database performance.

There was a challenge, however: MongoDB Atlas for Government was in the process of obtaining FedRAMP approval at the time of Utah's migration deadline. Fortunately, Gangwar's team found a way to keep MongoDB at the core of the solution. The department performed its first migration of eREP to self-managed Amazon Elastic Compute Cloud (EC2) instances to meet the state's deadline. Then, once the FedRAMP approval process was complete four months later, it migrated again to managed MongoDB Atlas for Government. "We didn't want to lose MongoDB as the backend database: we were adamant on that," said Gangwar. "So, we took the extra step of moving to EC2 just so we could retain MongoDB."

The department also used Cluster-to-Cluster Sync, a solution that enables seamless, long-running cross-cluster syncing of real-time data, to ensure the migration ran smoothly. As an early customer of the solution, the Utah team helped provide feedback to MongoDB as it tested and improved the functionality.

Key Takeaways:
Now that eREP is running on MongoDB Atlas for Government, it returns results 25% faster than it did when data was stored on premises. MongoDB Atlas can handle the multiple layers of files and document embedding that the State of Utah uses as well as the large file sizes. "MongoDB is so responsive. Other database solutions couldn't give us this functionality," said Gangwar. "For our caseworkers, when somebody is standing in front of them, they want the software to return results quickly and not just keep processing and processing."

Additionally, the migration created more efficiency for the department. "It's much less cumbersome to maintain our databases now that we're using fully managed MongoDB Atlas for Government," said Gangwar. Database architects no longer have to manage shards, configurations, or load balancing; they can spend their time on more important developments, such as upgrading the rule engine at the backend of the eREP solution. They can also expand their cloud skills and explore new ways to use technology to serve the people of Utah.

The application also has faster disaster recovery capabilities on MongoDB Atlas for Government. On premises, restoring the department's 10 TB backup could take up to 58 hours. Now, backups are automated, and restoring the databases in case of an outage takes less than five minutes. "We're so happy that point-in-time restore is possible on the new cloud solution," said Gangwar. "We have alerts in place if anything goes above threshold levels, and we don't need to maintain manual scripts or switch over clusters; it's all fully managed now."

The State of Utah will continue to work to provide improved access to public services. "As public servants, my team is passionate to do work that directly impacts people's lives," said Gangwar. "We're so delighted that with this work behind the scenes in IT, we're helping 3.2 million Utah citizens, and we're proud that MongoDB is with us as we help our customers."

"The reason we like working with MongoDB is their promptness," said Gangwar. "They went above and beyond to help us, and we worked together to solve any problems."

Scan the QR to view full success story

MongoDB.

The most versatile way for the U.S. public sector to deploy, run, and scale workloads in the cloud.

When government agencies need to modernize aging legacy databases, they look to MongoDB Atlas for Government-secure, fully managed, and FedRAMP-Authorized.

In today's complex and ever-changing digital landscape, ensuring robust security while maintaining operational flexibility is non-negotiable for government agencies and enterprises alike. MongoDB Atlas for Government is FedRAMP® Moderate Authorized, meeting the rigorous security standards required by U.S. governmental organizations.

Our dedicated platform supports use cases from transactional data processing to vector search, AI-powered applications, and petabyte-scale data storage, enabling seamless operations while protecting your critical information. Operated solely by U.S.-based MongoDB employees on U.S. soil, this environment ensures trusted compliance for government and regulated industries.

Discover why over 60,000 organizations trust MongoDB.

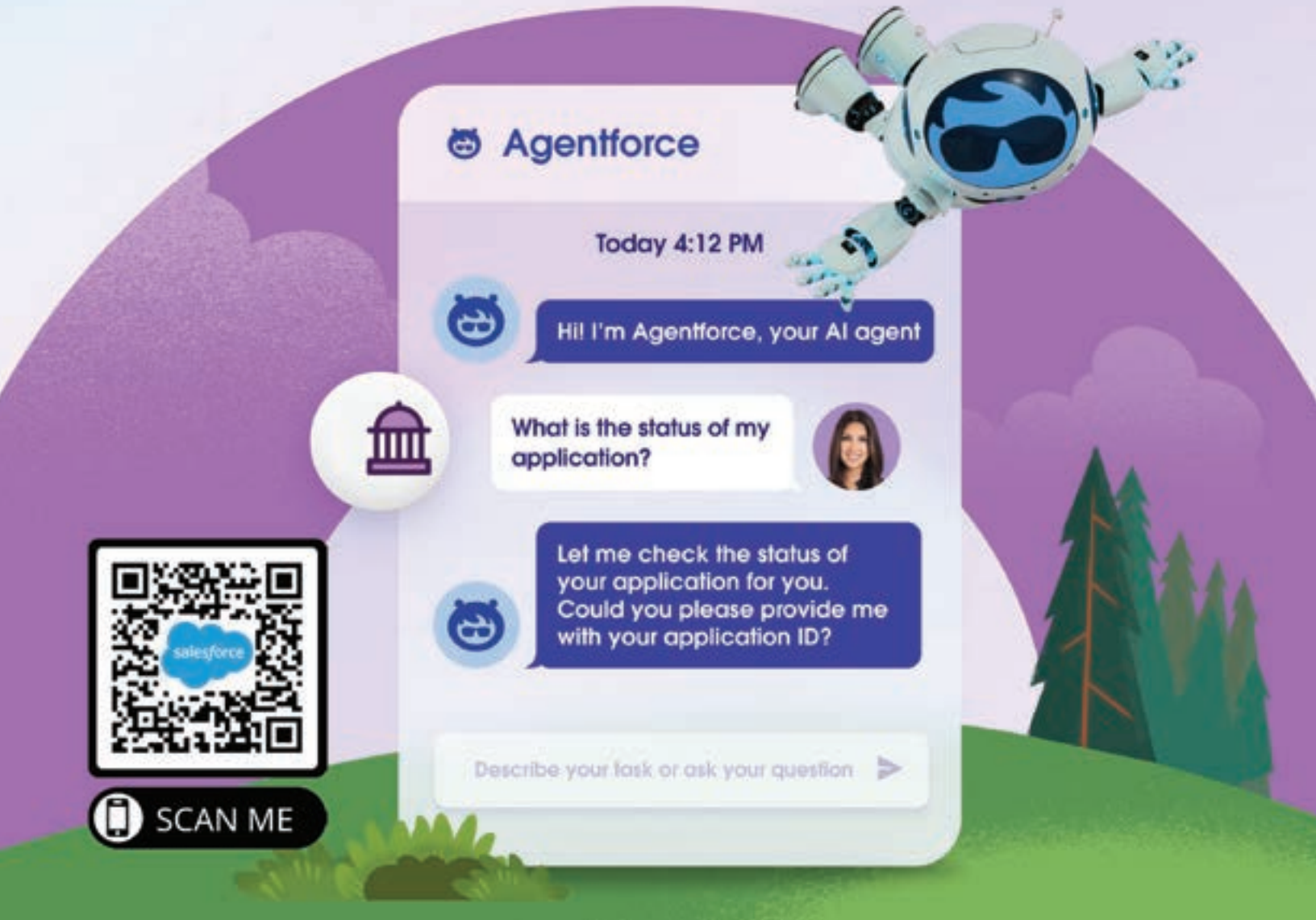
Secure your data with MongoDB Atlas for Government.

salesforce

Agentforce

Build public trust and connection with Agentforce for Public Sector

Learn how humans with AI agents can drive customer success together across public sector, higher education, and nonprofit industries.



USCIS Deploys an Enterprise-Wide, Data-Driven Platform That Unlocks Efficiencies Across Its Casework

U.S. Citizenship and Immigration Services (USCIS) launched the Director's Catalog on Salesforce Tableau --giving USCIS a portfolio of tools that staff can use to access data visualizations, pulling from one common, consistent, comprehensive data lake across DHS and sister agencies as appropriate. Learn how USCIS leverages a data-driven platform to enhance efficiency and support the American Dream.

The Challenge:

Like many Federal agencies, USCIS has no shortage of data, and the question is instead around how to make it accessible and usable. Which is where USCIS differs; unlike many Federal agencies, the USCIS team turned this into a call-to-action.

USCIS manages and adjudicates immigration cases across 90 field offices and five service centers for a variety of customers, ranging from more traditional groups (those looking to come to the U.S. on a work visa or pursue citizenship, for example), to migrant works, to those that are fall within humanitarian efforts, like those seeking to claim asylum or refugee status from war-torn regions.

The Solution:

The series of reports and dashboards USCIS, and teams deployed in order to do this serves a prime an example for any IT, program, or mission leaders looking to:

- Make their agency's data more available, accessible, or actionable across its case management programs and services
- Get people comfortable with using data in their day-to-day work
- Incorporate and share mission-critical data that might not be dispersed across the organization, as well as across sister agencies
- Leverage the benefits that come from strategic partnerships between IT and line of business

"Many people asked me to build them a report, and instead I said 'no, I'll go build you the platform that you can use to build your own reports,'" said Shawn Benjamin, Deputy Chief, Systems and Delivery Division, USCIS. "I don't care about their data as much as I care about enabling them to access their data. Because they are the experts in their business, IT can be most helpful if it can enable the business to unlock that expertise and make it easy for everyone to understand. That's what it means to democratize data."

In other words, the actions this team took did more than address common industry challenges in a proactive manner. They are building the foundation teams will need as the next wave of technological advancements mature to become the norm, establishing the model for success over the longer term.

Key Takeaways:

Since going live, the Directors Catalog has grown from 50 users to 15,900+ users and counting.

"It's amazing that USCIS espouses a culture of "data stewardship", recognizing that data doesn't belong to anyone. It's so amazing that we have eliminated that hurdle because that's time and energy we get to refocus on the people we welcome into the United States," said Beth Puchek, Chief Data Officer, USCIS. "It highlights the importance of having systems that can talk to one another, streamlining processes, and using good data to guide your mission."

RegScale

How NIWC PAC Slashed ATO and Onboarding Timelines with Compliance as Code

The U.S. Navy's Naval Information Warfare Center Pacific (NIWC PAC) used RegScale to automate their continuous cloud monitoring process and the six NIST RMF stages in their COSMOS platform. This breakthrough reduced NIWC's ATO timelines from 18+ months to rapid deployment while enabling fast adoption of new cloud technologies across the DoD.

The Challenge:

NIWC was facing a critical bottleneck. Traditional Authority to Operate (ATO) processes dragged on for over 18 months, burning through resources and blocking innovation. Manual compliance processes were choking progress, making programs inefficient, unreliable, and impossible to scale.

In response, NIWC proposed an ambitious vision: to establish secure government cloud (GovCloud) access with a commercial-like experience for research, development, engineering, and testing. At the same time, NIWC aimed to shift security left through automation and make every system/application component ATO-ready at the time of deployment.

The Solution:

NIWC PAC set out to revolutionize their approach to Government Cloud security and compliance. They needed a shift-left approach with compliance as code and self-updating documentation that could eliminate manual compliance work from the software development process. Their answer: the COSMOS (Cloud Operations, Security, Management and Optimization at Speed of Commercial) platform.

Within the COSMOS platform, RegScale delivers GRC outcomes faster and cheaper than any legacy program by:

- **Accelerating processes** while boosting visibility, quality, and reliability
- **Automating the RMF build-out,** monitoring, and System Security Plan (SSP) updates
- **Implementing real-time dashboards, reports,** and alerts for proactive security and compliance oversight with immediate issue resolution
- **Bridging the gaps between security, risk, and compliance** with extreme automation and Continuous Controls Monitoring

Key Takeaways:

Within COSMOS, RegScale provides the capability to enable GRC outcomes faster and cheaper than any legacy program. The transformation is dramatic:

- **Speed**
  ATO timelines slashed from 18+ months to rapid deployment
- **Efficiency**
  Minimized painful team handoffs and manual operations
- **Cost**
  Dramatically reduced program expenses through automation
- **Quality**
  Continuous monitoring ensures consistent security posture

As a result, COSMOS now provides the DoD with exactly what NIWC envisioned: commercial-speed cloud operations that maintain government-grade security.

Scan the QR to view full success story

RegScale

FedRAMP High

OSCAL FOUNDATION

Bridging security, risk, & compliance for government agencies

Achieve Continuous Authority to Operate (cATO), automate every step of the RMF, accelerate CMMC timelines, and embrace compliance as code with NIST OSCAL.

Accelerate ATO and deliver cATO

36+ weeks faster for Naval Information Warfare Center Pacific and 18-24 months faster for Marine Corps Community Services.

Streamline FedRAMP High

300% less time and **50% less cost** for package generation and submission.

Speed up your GRC program

Get rapid certifications for NIST 800-53, CMMC, and more. **Cut audit prep time by 60%.**

Cut authorization costs

$10M in delays and $100K per system per month saved by Operation StormBreaker USMCCS with automation.and efficiency.

Learn More **RegScale.com/industry-government/**

Axonius

Transform asset intelligence into *intelligent* action.

Preemptively tackle hard-to-spot exposures, misconfigurations, and operational challenges across your entire technology environment – all in one place.

The Axonius platform is FedRAMP Authorized

FedRAMP

Axonius

Axonius Asset Cloud: Cyber Asset Intelligence You Can Act On

Axonius Federal Systems is now FedRAMP Moderate Authorized, which unlocks a fully vetted, compliant path for agencies to adopt the Axonius Asset Cloud. Axonius helps federal teams modernize their cybersecurity to protect high-stakes missions, not just check boxes for compliance.

The Challenge:

Federal agencies face fragmented tools, siloed data, and rising compliance pressure. Security, IT, and compliance teams need fast answers to questions like:

- What assets do we have?
- Which are unmanaged, vulnerable, or noncompliant?
- How do we take action without adding complexity?

The Axonius Asset Cloud answers those questions.

The Solution:

The Axonius Asset Cloud is far more than an up-to-date asset inventory. It's an actionability platform designed to eliminate blind spots and reduce operational inefficiencies with capabilities that include:

- Providing real-time visibility into all assets, including shadow IT
- Detecting and remediating misconfigurations and policy drift
- Modernizing Continuous Diagnostics and Mitigation (CDM) reporting and analytics
- Enriching Continuous Monitoring and Risk Scoring (CMRS) program data
- Streamlining Cybersecurity Maturity Model Certification (CMMC) compliance
- Automating Zero Trust enforcement
- Generating audit-ready reports

Deployed via SaaS, on-prem, or private cloud, Axonius Federal Systems meets agencies where they are. We're already advancing toward FedRAMP High, Impact Level 5, and regional frameworks like GovRAMP and TX-RAMP. Our roadmap follows your challenges and removes what slows you down.

Key Takeaways:

With Axonius, you can stop proving you're secure and start being secure.

Trusted by 70+ Agencies. Data from 1,200+ tools. FedRAMP Moderate Authorized.

Scan the QR to view full success story

fm:systems

Washington County Maximizes Space Efficiency with OpenBlue Workplace

With a population of 267,000 residents, Washington County's mission is to provide excellent and cost-effective services that support healthy, peaceful, safe, and sustainable communities while encouraging meaningful participation in community activities and ensuring County governance. It has more than 1,300 employees who work across 26 buildings totaling nearly 1 million square feet.

The Challenge:

For many years, Washington County relied on an outdated legacy system that became increasingly challenging to use for space planning, managing their evolving workplace and assets, and employee experience needs. The existing system not only required heavy customization, which led to frequent inconsistencies and user errors, it also lacked intuitive design that ultimately discouraged the facilities and space planning team from using it all together.

When the County added a new property to its real estate portfolio, with plans to renovate and triple its size, the necessary upgrades to the existing system were exceptionally difficult that made it impossible to input the floor plan. Without having visibility into their workplace expansion project, it became highly cumbersome and time-intensive to research where facilities technicians were asked to make repairs, which rooms needed to be serviced, and to accurately track work orders for specific places without knowing where and when to follow up.

What's more, because everyone had different ways of tracking utilization data and technician work orders, data was inconsistent, and oftentimes required calling the customer support contact to export reports. The County also struggled with handling conditional formatting to allow for necessary security access requests for each department, since the IT, HR and Sheriff's department all had varying clearance requirements.

Lastly, the legacy system lacked effective data gathering for proactively managing preventive maintenance tasks. The County found themselves manually inputting and managing large numbers of equipment pieces that was equally time-consuming and inefficient. "The previous solution actually had the capability to provide digital floor plans, but we were unable to add our newest building's floor plan into the system." Whitney Libby, Project Specialist, Washington County.

The Solution:

Rather than make costly upgrades to a system that wasn't functioning, Washington County turned to OpenBlue Workplace for a reliable workplace management solution that could easily provide space planning for managing their existing and future space needs as well as effectively provide maintenance and asset management across their full real estate portfolio. When OpenBlue Workplace was selected as the IWMS vendor for Washington County, RSP Architects worked closely with Washington County to conduct a needs analysis of their current solution to ensure OpenBlue Workplace was set up to match the way the County needed it to function immediately, and in the future. This involved discovering what data was available from the legacy system, making sure the data was categorized correctly when transferring over to OpenBlue Workplace, and lightly configuring the new system for easy adoption.

Key Takeaways:

The switch to OpenBlue Workplace has significantly transformed the workplace management process for Washington County, providing a user-friendly and robust solution for easily managing, analyzing, and reporting on all their workplace, facilities and real estate operation and maintenance (O&M) data.

"OpenBlue Workplace is a highly regarded platform that helps thousands of organizations optimize their facilities and workplaces. For Washington County, having a completely integrated workplace management solution that was easy for people to use, could automate data gathering, and was scalable to grow with our changing needs was key."

Whitney Libby
Project Specialist, Washington County

Scan the QR to view full success story

fm:systems | Johnson Controls

Workplace Management Software for Government Agencies

- ✓ FedRAMP Authorized Solutions
- ✓ Meet & Exceed BIM Requirements
- ✓ Comply with Government Mandates

Learn More

DATADOG FOR GOVERNMENT

Built for Security. In-Process for FedRAMP® High.

Datadog helps federal agencies modernize securely with unified observability, real-time threat detection, and built-in compliance insights. With FedRAMP® Moderate Authorization and FedRAMP® High 'In-Process' status, Datadog is ready for mission-critical workloads across hybrid and multi-cloud environments.

How Datadog supports secure, efficient operations:

SECURITY-FIRST OBSERVABILITY
Built for mission-critical workloads

UNIFIED VISIBILITY
Monitor users, systems, and devices in real time

THREAT DETECTION
Correlate logs, metrics, and traces to stop threats fast

CLOUD COST CONTROL
Spot inefficiencies and optimize spend without sacrificing performance

AI-NATIVE MONITORING
Track LLMs, GPUs, and CPUs with security and compliance top of mind

See Datadog in action.
Visit our booth and read our press release at bit.ly/fedramphigh,
Contact fed@datadoghq.com to discuss your agency's mission needs.

DATADOG

DATADOG

ECCO Select Uses Datadog To Enhance USDA's Digital Capabilities and Meet FedRAMP® Requirements

USDA's DISC has been providing services as a federated data center since 1973 and performing data center migrations since the 1980s. It cross-services 14 federal departments and bureaus and supports 700 government-to-government agreements, leveraging inheritable enterprise standards in security, architecture, and procurement.

ECCO Select is a trusted Managed Services Provider (MSP) providing people, process, and technology solutions tailored to clients' needs. As an established federal contractor, talent acquisition, and advisory consulting company, ECCO Select offers top-tier IT experts and program management services.

The Challenge:

DISC's hybrid-cloud architecture delivers substantial efficiencies but also introduces challenges that could not be met with its legacy monitoring tool. A 2021 Executive Order also required the organization to deploy a FedRAMP®-authorized solution.

The Solution:

To meet DISC requirements, ECCO Select evaluated FedRAMP®-authorized monitoring and observability solutions and selected Datadog as its end-to-end observability platform, allowing it to monitor and manage all aspects of its IT environment, from its foundational infrastructure to the delivery of end-user experiences.

With Datadog in place, ECCO Select can offer essential managed services that provide real-time visibility into the health, performance, and configuration of IT services and assets. These systems are not only observable at a macro level by DISC, but individual tenants can use the platform's self-service features to securely access and monitor their specific infrastructure resources and applications. DevOps teams across DISC's portfolio of customers now have unified visibility into the health of their IT systems and can observe the performance of systems, servers, applications, and other resources within the enterprise technology stack.

Key Takeaways:

Within 75 days of the project start date, the ECCO Select team completed an automated deployment of the Datadog Agent to 4,800 hosts running in both on-prem data centers and cloud-hosted environments. This gave them full monitoring coverage of over 95 percent of their infrastructure, including around 4,000 containers as well as network and storage devices and databases. They were also able to seamlessly transition over 1,100 monitor templates, covering infrastructure services, logs, and synthetic tests, from the legacy monitoring system. This process was validated through a carefully phased approach to ensure accuracy and reliability.

"Datadog didn't just resolve a memory issue. It transformed DISC's entire approach to infrastructure monitoring."

Chris Condon
Director of Enterprise Observability, ECCO Select (Managed Services Provider to USDA)

Scan the QR to view full success story

US Government Agency Enhances Security and Reduces Risk with Tenable One Exposure Management Platform

A U.S. government agency significantly enhanced their cybersecurity posture by adopting the Tenable One Exposure Management Platform. Faced with increasing complexity across their IT landscape, the agency turned to Tenable to unify and strengthen its risk management efforts.

The Challenge:

Struggling with delayed identification of critical vulnerabilities, frequent false positives, and poor support from its existing provider, the agency found it increasingly difficult to maintain effective cyber resilience. These challenges limit the agency's ability to protect its globally distributed infrastructure and customer base.

With a rapidly growing and complex mix of on-premises and cloud assets, the agency needed a modern exposure management program. It required comprehensive visibility across all systems and a more efficient method to understand, assess, and report on risk exposure.

The Solution:

The Tenable One Exposure Management Platform was selected by the agency to unify and scale its capabilities. Tenable One offered complete visibility into the agency's attack surface, allowing them to efficiently assess and prioritize risk across all assets.

With Tenable One, the agency can scan its traditional IT assts, cloud workloads, containers, web applications, and Active Directory. Additionally, Tenable One provides consistent security policies, benchmarks, and reporting across on-premises and cloud environments. This has significantly improved the agency's ability to enforce standards, maintain compliance, and ultimately strengthen its overall security posture.

Key Takeaways:

- Strengthening security posture with scalable exposure management
- Enhanced visibility and support enabling risk prioritization
- Minimizing false positives and improving detection of vulnerabilities

tenable | carahsoft

Your exposure ends here.

Cyber risk solutions for federal, state and local governments

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for approximately 44,000 customers around the globe. See how Tenable can help your team expose and close the priority cyber weaknesses that put your agency at risk.

Visit Tenable.com for more information.

databricks | carahsoft.

A New Era in Public Sector Data Intelligence

Databricks Achieves FedRAMP High Authorization for AWS GovCloud

Listen Now >

Google Cloud

Powering Innovation: Google Cloud Expands FedRAMP High Portfolio

Google Cloud is committed to protecting sensitive agency data at the highest level of assurance within the FedRAMP program while also streamlining the adoption of secure and modern cloud technologies with continued **FedRAMP High authorizations** across our Data, AI, Infra and Collaboration solutions and services. FedRAMP High authorized services include:

- **Google Agentspace** brings powerful search and agentic capabilities to federal agencies.
- **Gemini in Workspace apps and the Gemini app** are the first generative AI assistants for productivity and collaboration suites to have achieved FedRAMP High authorization.
- **Google Workspace** including applications such as Gmail, Drive, Docs, and Calendar provides secure collaboration and productivity tools for federal agencies.

Many of these services, including Agentspace, are available through **Assured Workloads**, which provides the ability to configure sensitive workloads to meet stringent FedRAMP requirements. This expansion underscores Google's commitment to delivering secure and compliant AI solutions to the public sector.

SCAN
to Learn More

Carahsoft FedRAMP Portfolio

Carahsoft proudly represents over half of all FedRAMP-authorized vendors, showcasing our commitment to providing secure and compliant cloud solutions. This section highlights our FedRAMP portfolio, including those who are FedRAMP Authorized, In-Process, and Ready.

Scan the QR to learn more about Carahsoft's FedRAMP Solutions

CSP	Service Model	Impact Level	Authorization Status
22nd Century Technologies Inc.	SaaS	Moderate	In Process
Abnormal AI	SaaS	Moderate	Authorized
Absolute Security	SaaS	Moderate	Authorized
Acadis	SaaS	Moderate	Authorized
Acalvio Technology	SaaS	Moderate	Ready
Accellion USA, LLC.	SaaS	Moderate	Authorized
AchieveIt Online, LLC	SaaS	Low	Authorized
Acquia Inc.	PaaS	Moderate	Authorized
Actsoft, Inc	SaaS	Moderate	Authorized
Adobe	SaaS SaaS	LI-SaaS Moderate	Authorized Authorized
AINS dba OPEXUS	PaaS, SaaS	Moderate	Authorized
Akamai	IaaS	Moderate	Authorized
Alation	SaaS	Moderate	Ready
Altana	SaaS	High	In Process
Amazon	IaaS, PaaS, SaaS IaaS, PaaS, SaaS	Moderate High	Authorized Authorized
Appian	PaaS, SaaS PaaS, SaaS	Moderate High	Authorized Authorized
AppOmni	SaaS	Moderate	Authorized
Apptio an IBM Company	SaaS	Moderate	Authorized
Aqua Security Software Inc.	SaaS	High	Authorized
Armis Federal LLC	SaaS	Moderate	Authorized
Ask Sage, Inc.	SaaS	High	Authorized
Atlassian	SaaS	Moderate	Authorized
Authentic8, Inc.	SaaS	Moderate	Authorized
Autodesk	SaaS	Moderate	In Process

CSP	Service Model	Impact Level	Authorization Status
AutoRABIT Holding, Inc.	SaaS	Moderate	In Process
AvePoint Inc.	SaaS	Moderate	Authorized
Axiad IDS Inc.	SaaS	Moderate	In Process
Axon	SaaS	High	Authorized
Axonius Federal Systems	SaaS	Moderate	Authorized
Bamboo Health, Inc.	SaaS	Moderate	Authorized
Bentley Systems, Incorporated	SaaS	Moderate	In Process
BetterUp, Inc.	SaaS	Moderate	Authorized
BeyondTrust	SaaS	Moderate	Authorized
BlackBerry	SaaS	High	Authorized
Bluescape	SaaS	Moderate	Authorized
Bonterra	SaaS	Moderate	Ready
Boomi	SaaS	Moderate	Authorized
Box Inc.	SaaS	High	Authorized
Broadcom	SaaS SaaS	Moderate High	Authorized Authorized
Casepoint LLC	SaaS	Moderate	Authorized
Cellebrite	SaaS	High	Ready
ChargePoint, Inc.	SaaS	LI-SaaS	Authorized
Check Point Software Technologies, Inc.	SaaS	Moderate	In Process
Checkmarx	SaaS	High	Ready
Chronus LLC	SaaS	Moderate	Authorized
Cloudera Government Solutions, Inc	PaaS	Moderate	In Process
Code42	SaaS	Moderate	Authorized
Cofense	SaaS	Moderate	Authorized
Cohesity	SaaS	Moderate	Authorized

CSP	Service Model	Impact Level	Authorization Status
Collabware	SaaS	Moderate	Authorized
Collibra	SaaS	Moderate	Authorized
Commvault Systems, Inc.	SaaS	High	Authorized
Concur Technologies, Inc.	SaaS	Moderate	Authorized
Confluent Inc.	SaaS	Moderate	Ready
Copado	SaaS	Moderate	Authorized
CORAS	SaaS	High	Authorized
CoSo Cloud, LLC.	SaaS	Moderate	Authorized
Covergent Solutions Inc dba Exiger Government Solutions (EGS)	SaaS	Moderate	Authorized
CrowdStrike, Inc.	SaaS	Moderate	Authorized
CyberArk Software LTD	SaaS	High	Authorized
CyLogic	IaaS	High	Ready

Diligent

Automate Public Sector ITGRC with the Diligent One Platform

Why public sector leaders choose Diligent:

One platform for all GRC needs

Eliminate point solution sprawl. The Diligent One Platform consolidates cyber security, IT risk, compliance, and audit oversight into a centralized, scalable environment.

Actionable cyber security automation

Automate evidence collection, IT controls testing, and reporting to reduce time to compliance.

Integration-ready architecture

The Diligent One Platform connects with your existing security tools and infrastructure to enable continuous monitoring and real-time threat mitigation.

Unify federal and state GRC functions in a single platform.

Diligent One offers a single, unified platform to manage your entire ITGRC program – with FedRAMP Moderate and DoD IL5 authorizations meeting the highest federal security and compliance standards.

What sets Diligent apart?

- ✓ **Pre-built** framework content
- ✓ **Automated** workflows
- ✓ **Deadline-ready** implementation
- ✓ **Unified** compliance approach

Ready to simplify your ITGRC program?

Discover how the Diligent One Platform helps public sector CISOs accelerate compliance, mitigate risk, and modernize their GRC posture – all in one secure, intelligent platform.

CSP	Service Model	Impact Level	Authorization Status
Databricks, Inc.	SaaS PaaS, SaaS PaaS, SaaS	High Moderate High	In Process Authorized Authorized
Datadog	SaaS SaaS SaaS	LI-SaaS Moderate High	Authorized Authorized In Process
Decision Lens Inc.	SaaS	Moderate	Authorized
Digital.ai	SaaS	Moderate	Authorized
Diligent, Inc.	SaaS	Moderate	Authorized
Docebo	SaaS	Moderate	Authorized
DocketScope, Inc.	SaaS	Moderate	Authorized
DocuSign	SaaS	Moderate	Authorized
DOMA Technologies, LLC	SaaS	Moderate	Ready
Druva, Inc.	SaaS	Moderate	Authorized
DTEX Systems, Inc.	SaaS	Moderate	In Process
Dynatrace	SaaS	Moderate	Authorized
e-Builder, A Trimble Company	SaaS	Moderate	Authorized
eGain Corporation	SaaS	Moderate	Authorized
Egnyte Inc.	SaaS	Moderate	Ready
Eightfold AI Inc.	SaaS	Moderate	Authorized
Elastic	SaaS	Moderate	Authorized
ETHERFAX	IaaS	High	In Process
Everbridge	SaaS	Moderate	Authorized
Everfox	SaaS	Moderate	In Process
Exterro, Inc.	SaaS	Moderate	Authorized
ExtraHop Networks	SaaS	Moderate	In Process
FM:Systems	SaaS SaaS	LI-SaaS Moderate	Authorized Authorized

CSP	Service Model	Impact Level	Authorization Status
Forcepoint	SaaS	Moderate	Authorized
FormAssembly, Inc.	SaaS	Moderate	Ready
Genesys	SaaS	Moderate	Authorized
GitLab	SaaS	Moderate	Authorized
Google	IaaS SaaS IaaS, PaaS, SaaS	High High High	Ready Authorized Authorized
Govini	SaaS	High	Authorized
Granicus	SaaS	Moderate	Authorized
H20.AI for Government	SaaS	High	In Process
HackerOne	SaaS	LI-SaaS	Authorized
Hootsuite	SaaS	LI-SaaS	Authorized
Human Resources Technologies, Inc. (HRTec)	IaaS, PaaS	High	Authorized
Hypori, Inc.	SaaS	High	Authorized
IBM	IaaS SaaS SaaS IaaS, PaaS	High Moderate High High	Authorized Authorized In Process Authorized
IBM Envizi ESG Reporting	SaaS	LI-SaaS	Authorized
iBoss	SaaS	Moderate	Authorized
Icertis Inc.	SaaS	Moderate	Ready
ID.me	SaaS	Moderate	Authorized
Illumio, Inc.	SaaS	Moderate	Authorized
Infoblox	SaaS	Moderate	Authorized
Informatica LLC	SaaS	Moderate	Authorized
Iron Mountain	SaaS SaaS	Moderate Moderate	In Process Authorized
Ivanti	SaaS	Moderate	Authorized
Juniper Networks	SaaS	Moderate	Authorized

CSP	Service Model	Impact Level	Authorization Status
Keeper Security	SaaS	Moderate	Authorized
Keyfactor	SaaS	Moderate	In Process
Kiteworks USA, LLC	SaaS	High	Ready
Knightscope, Inc.	SaaS	Moderate	Authorized
KnowBe4, Inc.	SaaS	Moderate	Authorized
Koniag Government Services	SaaS	High	In Process
LaunchDarkly	SaaS	Moderate	Authorized
Level Access	SaaS	LI-SaaS	Authorized
LogicMonitor	SaaS	Moderate	In Process
Lookout, Inc.	SaaS	Moderate	Authorized
Lucid Software, Inc.	SaaS	Moderate	Authorized
Mark43, Inc.	SaaS	High	Authorized
Mastercard Cybersecurity	SaaS	Moderate	Ready
Mathematica Inc.	PaaS	Moderate	Authorized
MAXIMUS Inc.	SaaS IaaS, PaaS, SaaS	Moderate Moderate	Authorized Authorized
Menlo Security	SaaS	Moderate	Authorized

CSP	Service Model	Impact Level	Authorization Status
MicroFocus	SaaS	Moderate	In Process
Microsoft	SaaS SaaS IaaS, PaaS, SaaS	Moderate High High	Authorized Authorized Authorized
MongoDB	PaaS, SaaS	Moderate	Authorized
Moveworks	SaaS	Moderate	In Process
MuleSoft	PaaS	Moderate	Authorized
NEOGOV	SaaS	Moderate	In Process
NetDocuments Software, Inc.	SaaS	Moderate	Authorized
Netskope, Inc.	SaaS SaaS	Moderate High	Authorized Authorized
New Relic	SaaS	Moderate	Authorized
Nexthink	SaaS	Moderate	In Process
NICE CXone	SaaS	Moderate	Authorized
NinjaOne	SaaS	Moderate	In Process
Nintex	SaaS	Moderate	Authorized
Nuance	SaaS	Moderate	Authorized
Nucleus Security, Inc	SaaS	Moderate	Authorized
Odaseva	SaaS	Moderate	Ready
Okta	SaaS SaaS	Moderate High	Authorized Authorized
OnSolve LLC	SaaS	Moderate	Authorized
Onspring Technologies, LLC	SaaS	Moderate	Authorized
OpenText	SaaS	Moderate	Authorized
Oracle	IaaS IaaS SaaS SaaS IaaS, PaaS IaaS, PaaS, SaaS	Moderate High Low Moderate High Moderate	Authorized Authorized Authorized Authorized Authorized Authorized

Microsoft | carahsoft.

Transformative Cloud

Azure for U.S. Government offers advanced compute and analytics from cloud to edge, empowering national security, intelligence, federal, state, and local agencies with the tools to accelerate their missions and deliver superior citizen services.

carah.io/MicrosoftTransformativeCloud

CSP	Service Model	Impact Level	Authorization Status
Orca Security	SaaS	Moderate	Authorized
OwnBackup	SaaS	Moderate	Authorized
PagerDuty	SaaS	Low	Authorized
Palantir Technologies	SaaS SaaS PaaS, SaaS	Moderate High High	Authorized Authorized Authorized
Palo Alto Networks, Inc.	SaaS SaaS	Moderate High	Authorized In Process
Paperless Innovations, Inc.	SaaS	Moderate	Authorized
Paramify	SaaS	High	Ready
Precisely Software	SaaS	Moderate	In Process
Procore Technologies, Inc	SaaS	Moderate	In Process
Profit Apps Inc	SaaS	Moderate	Ready
Project Hosts Inc.	PaaS PaaS	Moderate High	Authorized In Process
Proofpoint, Inc.	SaaS	Moderate	Authorized

CSP	Service Model	Impact Level	Authorization Status
PTFS/Liblime	SaaS	Moderate	In Process
Qlik Technologies Inc.	SaaS	Moderate	Authorized
Qualtrics, LLC	SaaS	Moderate	Authorized
Qualys	SaaS SaaS	Moderate High	Authorized In Process
Quzara, LLC.	SaaS	High	Ready
Rackspace Government Solutions	PaaS	Moderate	Authorized
Ramp	SaaS	Moderate	Ready
Rapid7	SaaS	Moderate	Authorized
Red Hat	PaaS	High	Authorized
RegScale	SaaS	High	Authorized
Rescale	PaaS, SaaS	Moderate	Authorized
RSA Security LLC	SaaS	Moderate	Authorized
Rubrik	SaaS	Moderate	Authorized
SailPoint Technologies, Inc.	SaaS	Moderate	Authorized
Salesforce	PaaS, SaaS	High	Authorized
SAP National Security Services Inc. (SAP NS2)	SaaS PaaS, SaaS	Moderate Moderate	Authorized Authorized
Saviynt, Inc.	SaaS	Moderate	Authorized
Scale AI, Inc	SaaS	High	Authorized
ScienceLogic, Inc.	SaaS	Moderate	Authorized
Second Front Systems	PaaS	High	In Process
SecurityScorecard, LLC	SaaS	Moderate	Ready
SentiLink Corp	SaaS	Moderate	Ready
SentinelOne	SaaS	High	Authorized
ServiceNow	PaaS, SaaS	High	Authorized

CSP	Service Model	Impact Level	Authorization Status
Skyhigh Security	SaaS	High	Authorized
Slack Technologies	SaaS SaaS	Moderate High	Authorized Authorized
Smartsheet	SaaS	Moderate	Authorized
SMX (Formerly Smartronix)	PaaS	Moderate	Authorized
Snowflake Inc.	SaaS SaaS	Moderate High	Authorized Authorized
Snyk	SaaS	Moderate	Authorized
Socure, Inc.	SaaS	Moderate	Authorized
Software AG Government Solutions	PaaS	Moderate	Authorized
Splunk	SaaS SaaS SaaS	Moderate Moderate High	In Process Authorized Authorized
Sprinklr, Inc.	SaaS	LI-SaaS	Authorized
StackArmor	SaaS SaaS	Moderate High	Authorized Ready
Steel Patriot Partners	SaaS	Moderate	Ready
Sumo Logic	SaaS	Moderate	Authorized
Synack	SaaS	Moderate	Authorized
Talkdesk	SaaS	Moderate	Authorized
Tanium	SaaS	Moderate	Authorized
Telos Corporation	SaaS	High	Authorized
Tenable	SaaS	Moderate	Authorized
ThreatConnect	SaaS	Moderate	Authorized
TransUnion	SaaS	Moderate	Ready
Trellix	SaaS	Moderate	Authorized
Trello	SaaS	LI-SaaS	Authorized
Trend Micro Inc.	SaaS	Moderate	Authorized


uberether
Launch your FedRAMP & DoD listing faster.
Engineered for mission speed.
UberEther.com/ATO
Instant Readiness
Reduce ATO Cost by 60-75%
Live threat alerts & reporting
Hyper secure enviornments

CSP	Service Model	Impact Level	Authorization Status
Trustwave Government Solutions	SaaS	Moderate	Authorized
Tyler Federal, LLC	PaaS, SaaS	Moderate	Authorized
Tyler Technologies Data & Insights	SaaS	Moderate	Authorized
UberEther	SaaS	High	Authorized
UiPath	SaaS	Moderate	Authorized
Unqork, Inc.	SaaS	Moderate	Authorized
Valimail	SaaS	LI-SaaS	Authorized
Vanta	SaaS	20x Low	In Process
Varonis	SaaS	Moderate	Authorized
Veracode	SaaS	Moderate	Authorized
Verint	SaaS	Moderate	Ready
Veritas Technologies, LLC	SaaS	Moderate	Ready
Veritone, Inc.	SaaS	Moderate	Authorized
Verkada Inc	SaaS	Moderate	Ready
Virtru	SaaS	Moderate	Authorized
VMware, Inc.	IaaS	High	Authorized
Vyopta Incorporated	SaaS	LI-SaaS	Authorized
WalkMe, Inc	SaaS	Moderate	Ready
Wasabi Technologies	SaaS	Moderate	Ready
WellHive Holdings, LLC	SaaS SaaS	Moderate High	Authorized In Process
WillCo Tech	SaaS	Moderate	Authorized
Wiz, Inc.	SaaS	Moderate	Authorized
Wolters Kluwer	SaaS	Moderate	Authorized
Workiva	SaaS	Moderate	Authorized

CSP	Service Model	Impact Level	Authorization Status
Zeva Incorporated	SaaS	Moderate	In Process
Zimperium	SaaS	Moderate	Authorized
ZL Technologies, Inc.	SaaS	Moderate	In Process
Zoom Video Communications, LLC	SaaS	Moderate	Authorized
Zscaler, Inc.	SaaS SaaS	Moderate High	Authorized Authorized

Onspring FedRAMP

Cloud-based, No-Code

GRC Software for Federal Agencies

Manage OMB A-123, POA&M, NERC & Policies with the #1 GRC software in the FedRAMP marketplace.

Learn how Onspring GovCloud can modernize your agency's governance, risk and compliance processes. Schedule your personalized demo today.

Onspring.com/GovCloud

zoom *for* Government

FedRAMP

Zoom for Government is a FedRAMP Authorized SaaS service operating at the Moderate baseline and has reciprocity to DoD Impact Level 2.

- Zoom Meetings
- Zoom Phone
- Zoom Team Chat
- Zoom Contact Center
- Zoom Webinars
- Zoom Rooms

...and so much more.

Interested in a briefing or quote?
Contact Zoom@carahsoft.com

zoomgov.com

Contract Vehicles

Carahsoft & our Reseller Partners offers a number of contract options for purchasing FedRAMP solutions. Our contracts offer purchasing options for civilian, defense, state, and local government customers. Customers can purchase solutions off of four major contract vehicles:

GSA Multiple Award Schedule (MAS)

Carahsoft & our Reseller Partners hold GSA Multiple Award Schedule's (MAS) that allow customers to procure a wide variety of FedRAMP solutions. Carahsoft holds Contract #47QSWA18D008F and allows customers to purchase everything from AI infrastructure to advanced analytics solutions.

2GIT

GSA's 2nd Generation Information Technology Blanket Purchase Agreements (2GIT BPAs) provide access to Commercial Off-The-Shelf (COTS) hardware/software and ancillary services. Carahsoft holds Contract #47QTCA21A000R to support the U.S. Air Force and all public sector customers.

ITES-SW2

The purpose of the ITES-SW 2 acquisition is to support Army, Department of Defense (DoD) and all Federal Agency enterprise Information Technology (IT) infrastructure and info-structure goals by leveraging Commercially availableOff-The-Shelf (COTS) software products and maintenance in 14 product categories in addition to related incidental services and hardware.

NASA SEWP V

The NASA SEWP V GWAC (Government-Wide Acquisition Contract) provides the latest in Information Technology (IT) products and product-based services for all Federal Agencies. SEWP provides the best value and cost savings through innovative procurement tools and processes; premier customer service and outreach; and advocation of competition and cooperation within the industry.

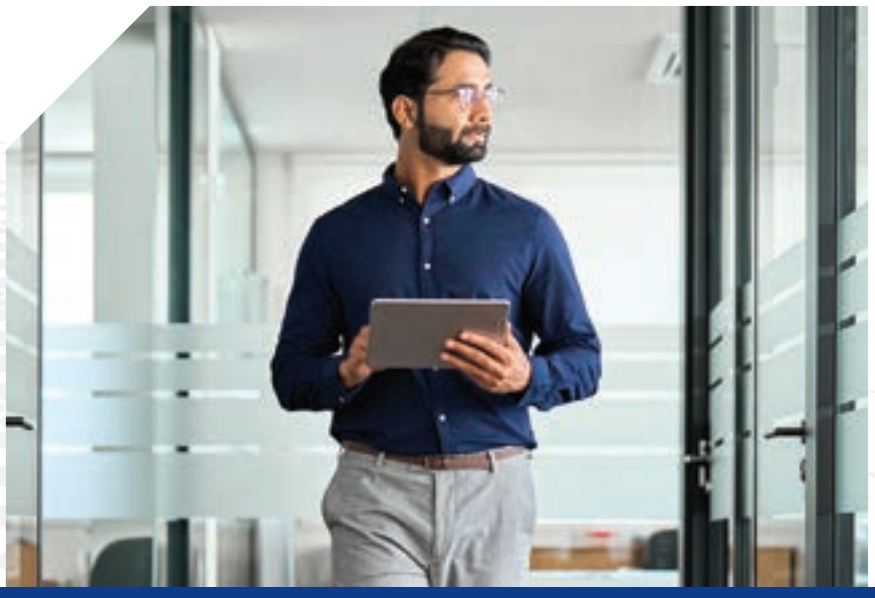
NASPO ValuePoint Cooperative Purchasing Organization

The NASPO ValuePoint Cooperative Purchasing Organization (formerly WSCA-NASPO) provides the highest standard of excellence in public cooperative contracting. By leveraging the leadership and expertise of all states with the purchasing power of their public entities, NASPO ValuePoint delivers best value, reliable, competitively sourced contracts.

Since 1993 NASPO ValuePoint has been the cooperative purchasing arm of NASPO (the National Association of State Procurement Officials) encouraging, fostering and guiding the nation's most significant public contract cooperative. NASPO ValuePoint is a unified, nationally focused cooperative aggregating the demand of all 50 states, the District of Columbia and the organized US territories, their political subdivisions and other eligible entities spurring best value, innovation and competition in the marketplace.

Explore the benefits of how you can count on Carahsoft and our Reseller Partners

- 24x7 availability call us at 888-662-2724
- Dedicated support specializing in serving enterprise ready solutions
- Ecosystem of value-added reseller partners
- Contract Expertise: We understand your procurement needs and the outcomes you're seeking
- Quick turnaround quote: Get the IT solutions you need with the fast, accurate service you deserve
- Substantial cost savings on Zero Trust products and service portfolio from certified technology brand partners
- Advanced technology solutions including development tools, agile planning, build & test, application deployment, continuous integration (CI/CD), cloud providers and more



carahsoft

Contact Us:

(888) 662-2724
FedRAMP@Carahsoft.com

11493 Sunset Hills Road, Suite 100
Reston, Virginia 20190

carahsoft.com/solve/fedramp