carahsoft The Trusted Education IT Solutions Provider®

FedRAMP Buyer's Guide for Cloud Service Providers

Navigating Cloud Security Standards: Insights and Benefits for CSPs in Achieving a FedRAMP ATO

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:

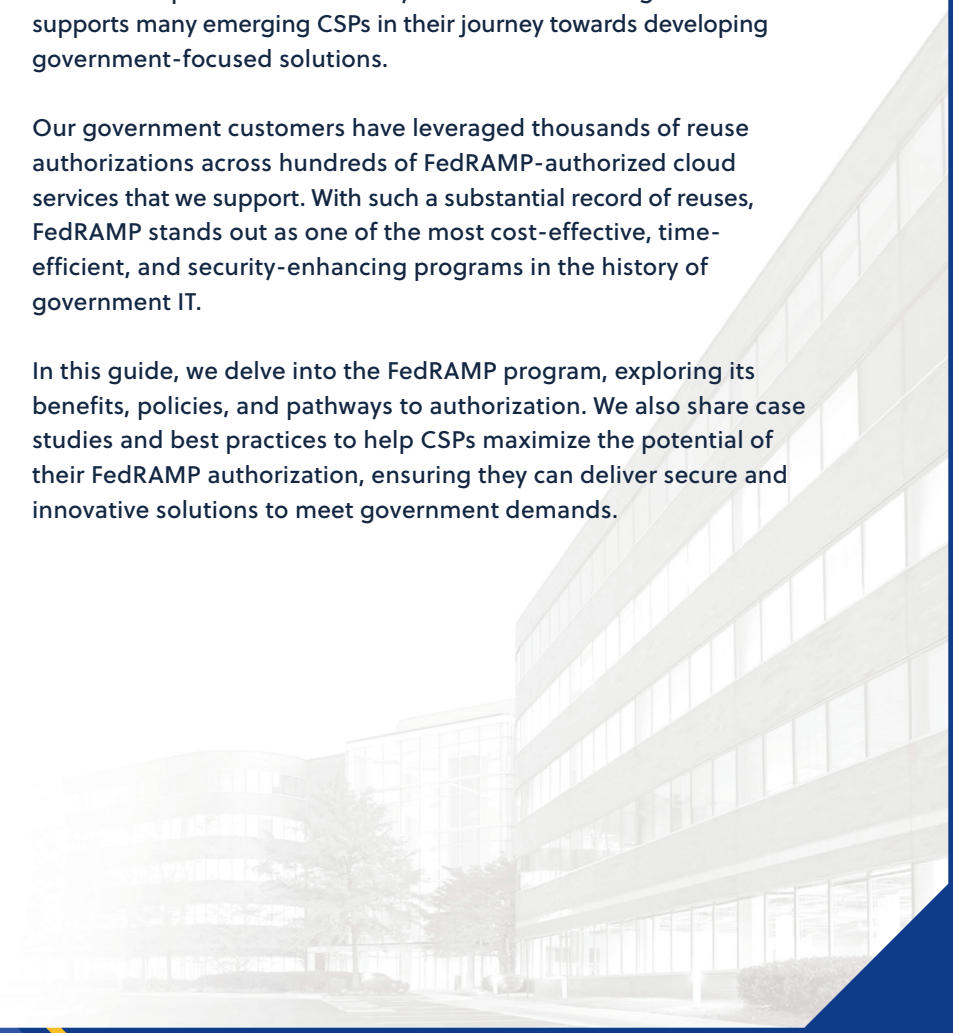
Welcome to the FedRAMP Buyer's Guide for CSPs!

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 Cloud Service Providers (CSPs), this is not just a valuable opportunity to align with the evolving needs of government customers – it is a mandatory requirement for delivering cloud solutions to Federal agencies.

Carahsoft represents a wide array of FedRAMP offerings and supports many emerging CSPs in their journey towards developing government-focused solutions.

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.

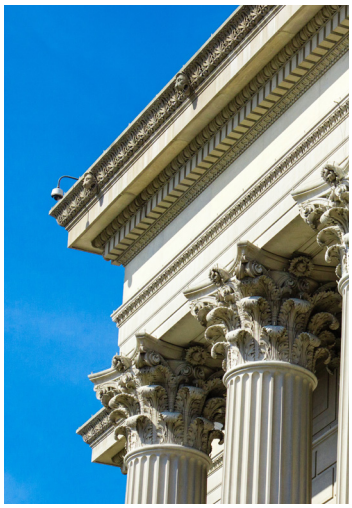
In this guide, we delve into the FedRAMP program, exploring its benefits, policies, and pathways to authorization. We also share case studies and best practices to help CSPs maximize the potential of their FedRAMP authorization, ensuring they can deliver secure and innovative solutions to meet government demands.



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)

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.*

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.

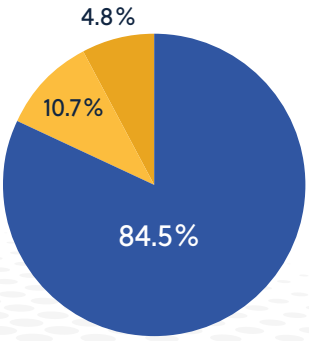
In Process

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

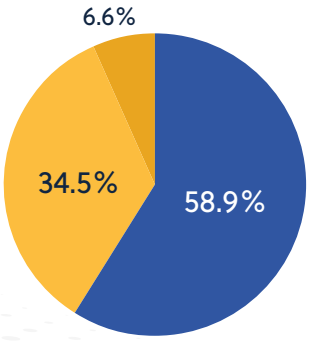
The CSO has successfully completed the FedRAMP Authorization process and the FedRAMP PMO has signed a FedRAMP ATO. This designation indicates that the FedRAMP compliance requirements have been met and the security package is available for agency reuse.

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



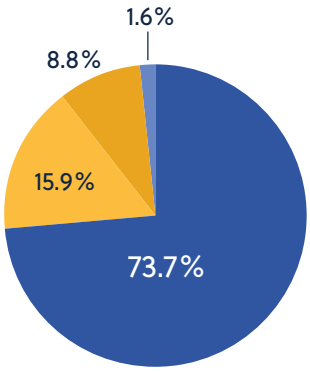
CSO by Service Model Type

- SaaS
- PaaS
- IaaS



CSO by Deployment Model

- Gov. Community Cloud
- Public
- Hybrid



CSO by Impact Level

- Moderate
- High
- LI-SaaS
- Low

Get the Most Out of Your FedRAMP Authorization

Achieving FedRAMP authorization unlocks a plethora of opportunities and benefits for CSPs. Understanding and leveraging these benefits can enhance market reach and credibility in both Federal and Commercial sectors.

FedRAMP for Federal Customers

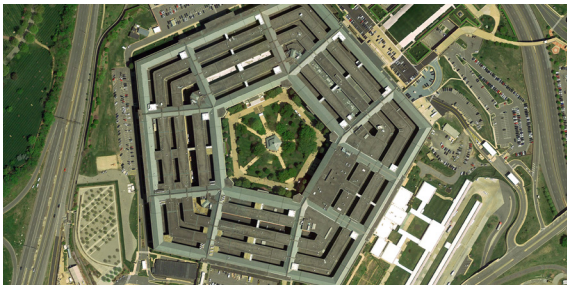
FedRAMP authorization enables your cloud services to be reused across multiple Federal agencies, unlocking significant opportunities with the Federal space. FedRAMP continues to grow at a steady pace, reflecting its increasing importance and value. The impact of FedRAMP's growth is evident in the number of reuse authorizations. In FY22, Federal agencies reused FedRAMP authorized products over 4,500 times, representing a 60% increase from FY21 and a 132% increase from FY20. These figures highlight the rising demand for secure, FedRAMP compliant solutions and the expanding market potential for vendors.

FedRAMP for Commercial & Healthcare

Today's landscape of heightened cyber threats has led commercial customers in cyber-vulnerable sectors, such as finance and healthcare, to recognize the value of FedRAMP's rigourous security standards. These customers are often willing to pay a premium for FedRAMP authorized versions of cloud products, knowing they will meet stringent government security requirements. Additionally, organizations engaged in federal contracts may be required to integrate FedRAMP authorized solutions into their operational framework, making FedRAMP authorization a crucial differentiator.

Growing Cloud Adoption in Government

The Federal Government continues to expand its adoption of cloud technologies, driven by the need for efficient, scalable, and secure solutions. CSPs with a FedRAMP authorization are well-positioned to capitalize on this growing demand, offering trusted and compliant solutions that meet the evolving needs of Government agencies.



DoD & GovRAMP Reciprocity

FedRAMP authorization can also facilitate entry into other government markets. The GovRAMP Fast Track Program offers a streamlined process for FedRAMP vendors to achieve GovRAMP authorization designation, enhancing marketability to State and Local Governments. Furthermore, there is direct reciprocity between the FedRAMP Moderate baseline and Department of Defense Cloud Computing Security Requirements Guide (DoD CC SRG) Impact Level 2 (IL2), allowing for easier transitions between Civilian and Defense markets.

Success Stories

Cloud Service Providers across industries are achieving FedRAMP authorization faster and more efficiently by partnering with Carahsoft's vendor ecosystem. Explore how others have successfully navigated the FedRAMP process and scaled their solutions for the federal market with the support of our trusted technology partners.

RegScale

FedRAMP High at Half the Cost: How a Small SaaS Company Cracked the Code in 6 Months

RegScale achieved a coveted FedRAMP® High Approved status with agency sponsorship from the Department of Homeland Security. Using our own AI-driven Continuous Controls Monitoring solution, we completed the entire process in 6 months for less than half the typical cost.

The Challenge:

If you're a company selling cloud services to the US federal government, you know that achieving a FedRAMP (Federal Risk and Authorization Management Program) High designation is more than a gold star — it's a critical requirement and a major competitive advantage. It's also a remarkable achievement, almost unheard of for a Series A startup operating with a limited staff and budget, that we set our sights on.

Even with enterprise-level resources, preparing the package for a FedRAMP Authority to Operate (ATO) typically takes 18 to 24 months, costs approximately $2 million, and requires arduous manual documentation. We needed to forge a faster, more cost-effective path to FedRAMP High with our small but mighty security team and our AI-driven automation platform.

The Solution:

To automate and accelerate the FedRAMP process, RegScale turned to its own Continuous Controls Monitoring (CCM) platform. Our solution helped us drastically streamline manual tasks like writing compliance packages and gathering evidence with a small team and limited resources. Leveraging our AI Author feature, we were able to see documentation gaps in a single pane of glass and draft control implementation statements that were already 80-85% complete upon initial generation.

Key Takeaways:

With the help of our own platform, we received our FedRAMP High ATO in just one-quarter of the average time and at 50% of the average cost. Using AI Author, we were able to write a package of 410 controls in just 2 weeks, a process that typically takes 12-16 weeks.

These results demonstrate that with the right technology and approach, even resource-constrained companies can navigate complex compliance requirements and unlock opportunities with the world's largest buyer, the US federal government. RegScale has proven that FedRAMP High certification is not just reserved for large enterprises — and we're proud to be paving the way for other innovative companies to follow suit.

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.

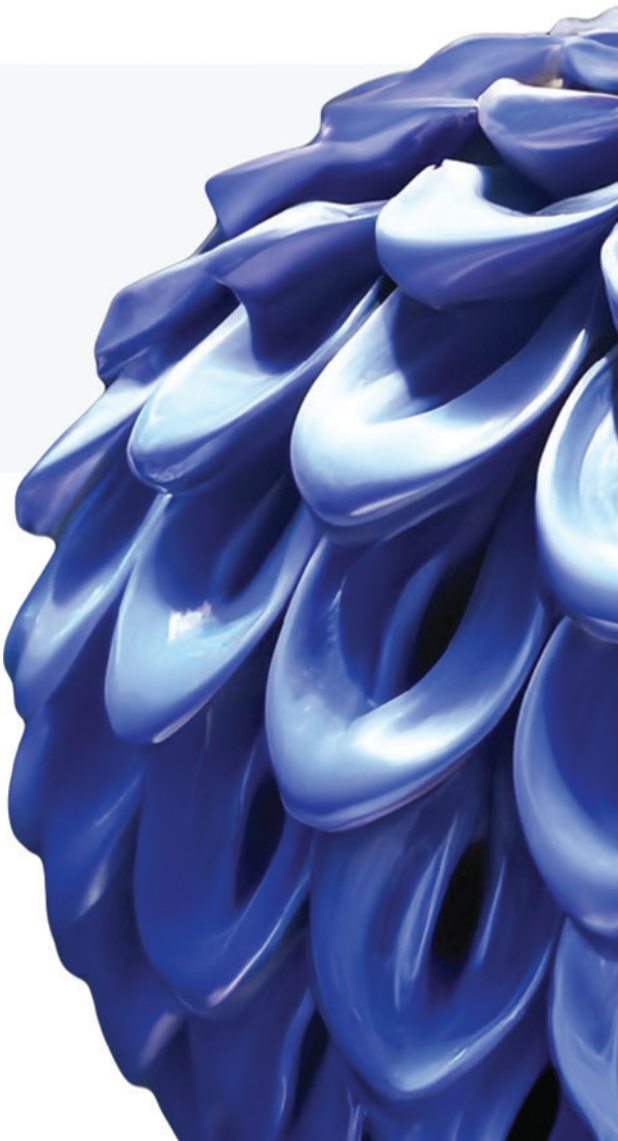
Learn More **RegScale.com/industry-government/**

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

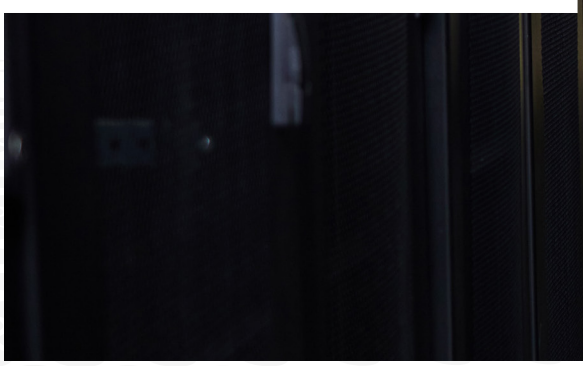
CSP	Service Model	Impact Level	Authorization Status
PTFS/Liblime	SaaS	Moderate	In Process
Qlik Technologies Inc.	SaaS	Moderate	Authorized
Qualtrics, LLC	SaaS	Moderate	Authorized
Qualys	SaaS SaaS	Moderate High	Authorized In Process
Quzara, LLC.	SaaS	High	Ready
Rackspace Government Solutions	PaaS	Moderate	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

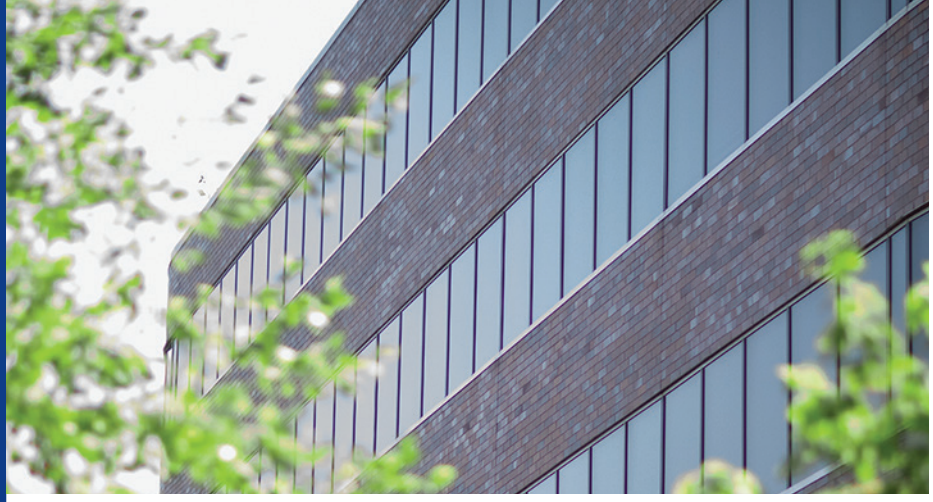
CSP	Service Model	Impact Level	Authorization Status
Skyhigh Security	SaaS	High	Authorized
Slack Technologies	SaaS SaaS	Moderate High	Authorized Authorized
Smartsheet	SaaS	Moderate	Authorized
SMX (Formerly Smartronix)	PaaS	Moderate	Authorized
Snowflake Inc.	SaaS SaaS	Moderate High	Authorized Authorized
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





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