AUTHORIZATION AS A SERVICE
GOVPOINT CLOUD SERVICES®

MIS Sciences Corporation – FedRAMP Cloud Service Provider FedRAMP (originally JAB) P-ATO (IaaS/PaaS/SaaS)

July 2025 (supersedes all previous versions)
v 2.6

MIS Sciences Corporation • 2550 N Hollywood Way • Suite 404 • Burbank, CA 91505
818.847.0213 • 877-262-3923
info@mis-sciences.com • www.mis-sciences.com

Contents

Abstract

MIS Sciences Corporation (MIS) is a FedRAMP-authorized Cloud Service Provider (CSP) for IaaS, PaaS, and SaaS, with a FedRAMP Provisional Authorization to Operate (P-ATO). Notably, GovPoint Cloud Services was initially authorized in 2016 by the FedRAMP Joint Authorization Board (JAB). MIS offers FedRAMP-authorized cloud services through GovPoint Cloud Services (GCS).

Without FedRAMP authorization, offering a cloud service or application to the Federal Government is challenging, if not impossible. Obtaining FedRAMP authorization is both expensive and time-consuming. It requires sponsorship from a federal agency, can cost up to $21.5 million, and typically takes 12 to 24 months to achieve.

Authorization as a Service (AaaS) provides a pathway for companies to obtain FedRAMP authorization for their products by joining the MIS GovPoint Cloud Services suite of FedRAMP-authorized offerings. Your offering can receive FedRAMP authorization within a matter of weeks.

As a Small Business Administration (SBA) Woman-Owned Small Business, MIS also opens up additional government opportunities for selling products, services, or solutions.

For more information:
MIS Sciences Corporation 818-847-0213
sales@mis-sciences.com
www.mis-sciences.com

GovPoint Authorization as a Service Overview

FedRAMP has become mandatory for selling to the Federal Government and many state governments. MIS Sciences Corporation has received a FedRAMP Provisional Authority to Operate (P-ATO) for its GovPoint Cloud Services, which include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). It's important to note that the FedRAMP Joint Authorization Board (JAB) initially authorized MIS GovPoint Cloud Services.

Unfortunately, obtaining FedRAMP authorization can be difficult for many companies because a sponsoring agency is mandatory under the new FedRAMP guidelines. The process can cost over $1.5 million and take between 12 and 24 months to complete, in addition to ongoing monthly expenses, making FedRAMP Authorization inaccessible for most companies.

MIS is actively seeking companies with services and applications they wish to provide to the Government that have a high probability of success in the Federal Government procurement process. If MIS accepts the vendor's service offering and the onboarding process is successfully completed, the vendor will be able to offer a FedRAMP-authorized version of their product or service to the Government.

Your product, service, or offering will be authorized under the MIS GovPoint Cloud Services FedRAMP Provisional Authority to Operate (P-ATO).

What types of offerings will MIS consider for Authorization as a Service?

MIS accepts three offerings: hardware and physical appliances, software and virtual appliances, and Extended Boundary. Each has different requirements and involves various processes.

Hardware and Appliances

The offerings include storage, specialized computing, and tailored environments such as AIX, HPC, and Security. These offerings are components of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and cannot function as standalone services. They must be part of a comprehensive IaaS environment, which MIS provides.

As components of IaaS, they must adhere to all applicable NIST 800-53 Rev 5 controls.

Software Applications and Virtual Appliances (SaaS)

Offerings include any application designed for end-users to perform specific tasks, such as accounting, security, development, human resources, management, and more—essentially, anything that supports business operations.

As a Software as a Service (SaaS) application, it must adhere to all relevant NIST 800-53 Rev 5 controls. The application can inherit applicable controls from the underlying FedRAMP Authorized Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

Extended Boundary

An Extended Boundary refers to a dedicated infrastructure environment designed for specific purposes, such as storage pods, specialized computing environments, or customer environments, requiring FedRAMP authorization. These Extended Boundaries are typically hosted in commercial data centers and must adhere to strict FedRAMP security controls.

As an Infrastructure as a Service (IaaS) component, an Extended Boundary is required to comply with all applicable NIST 800-53 Rev 5 controls. Once it receives approval, it becomes part of the MIS GovPoint Cloud Services FedRAMP authorization boundary.

How to use Authorization as a Service

Initial Evaluation

Contact MIS Sciences for an initial evaluation to see if your service or offering is a good fit for further consideration. MIS will discuss the requirements and associated fees.

Hosting requirement

(NOTE: Does not apply to Extended Boundary implementations)

The vendor's hardware, application, or service must be hosted within the MIS FedRAMP infrastructure to ensure the inheritance of all necessary underlying NIST 800-53 security controls. This requirement is essential for enabling Authorization as a Service.

The version of the hardware, application, or service must be the one provided to FedRAMP clients.

The application or services may be hosted on another FedRAMP-authorized platform, such as AWS, Azure, or a private data center.[1]

Security Evaluation

Software Applications and Virtual Appliances

MIS requires vendors to configure a production version of their application within the MIS Test Environment or another approved setting. The application must be fully functional, including all components and features that will be offered to end users.

MIS will conduct a security and compliance evaluation to assess FedRAMP compliance and identify deficiencies. Following this evaluation, MIS will provide the vendor with a list of identified vulnerabilities and deficiencies, along with recommendations for remediation. In certain circumstances, an assessment or penetration test by a 3PAO may be required before an offering is included as authorized.

Hardware Appliances

MIS requires vendors to configure their hardware appliances within the MIS Test Environment. This configuration must include all hardware and networking components, operating systems, and applications available to end users.

Similar to the software evaluation, MIS will conduct a security and compliance evaluation to assess FedRAMP compliance and identify potential weaknesses. The

[1] The application or services may be hosted on another FedRAMP-authorized platform, such as AWS, Azure, or a private data center.

vendor will receive a list of vulnerabilities and weaknesses, along with recommendations for remediation.

Before onboarding, the vendor must resolve all critical, high, and moderate issues, as well as any identified compliance deficiencies.

Extended Boundary

MIS requires a gap analysis of FedRAMP security controls and a pre-assessment of the infrastructure and data center. A 3PAO must conduct this assessment to identify any issues and compliance deficiencies.

Onboarding

Host Your Application or Hardware (This does not apply to Extended Boundary)

Host your application or hardware at MIS within the GCS FedRAMP environment or other FedRAMP environments (if MIS approves). Ensure the application or hardware is fully configured for production, as the client will use it. Please note that this step does not grant independent FedRAMP authorization; your application or hardware is only part of the MIS GCS FedRAMP environment and is not authorized until the Authorization as a Service process has been completed and approved.

Documentation

Working with MIS, completing the security analysis documentation, working with the MIS 3PAO for any assessments, and including the application in the MIS FedRAMP Marketplace services offering.

Optionally, you may also complete the documentation to allow MIS to add the services or applications to their GSA MAS IT 70 schedule.

Market Your FedRAMP Offering

You can market your offering as a FedRAMP authorized product. When marketing, you can state that a FedRAMP version of your product is available from your company or a reseller. Your offering will be listed as an authorized service under the MIS GovPoint FedRAMP Marketplace listing.

Optionally, your product or offering will be listed in the MIS GSA IT 70 MAS along with the price to the Government and discounts offered. Customers can order directly from the MIS GSA IT 70 MAS via their normal ordering process.

Fees and Costs

The fees and costs for participating in the MIS Sciences FedRAMP partner program depend on the type and complexity of the offering. Contact MIS for the current fee schedule.

About MIS Sciences Corporation

MIS Sciences Corporation (MIS) is an SBA-certified Woman-Owned Small Business and a GSA IT-70 contractor. Established in 1996, MIS has provided managed services to the public and private sectors, serving as a subcontractor on many large contracts.

MIS offers Managed Services, Dedicated Hosting, Cloud Services, and FedRAMP cloud services.

In 2014, MIS started the FedRAMP process and, in 2016, was awarded a JAB FedRAMP P-ATO at the moderate level for IaaS, PaaS, and SaaS. MIS is the only small business with a FedRAMP IaaS.

MIS does not leverage or inherit services from any other ISP or CSP. MIS manages its data facilities in Burbank, CA, and Las Vegas, NV. MIS owns all the Infrastructure and hardware, allowing it to provide specialized and custom environments to its clients.

Notes:

- This document is informational only and implies no guarantees or warranties regarding any service or statement.
- Any ATO issued by any agency for the partner offering or service shall be issued to MIS Sciences Corporation, GovPoint Cloud Services.
- MIS Sciences makes no representations or warranties regarding any vendor's product or offering regarding its inclusion in the GCS FedRAMP ATO.
- If the vendor fails to remediate any Critical, High, or Moderate finding within FedRAMP guidelines, MIS may discontinue and disconnect the vendor's services from the GCS network without notice.
- Failure to pay the monthly fees will result in the termination of service.
- Prior assessments or FedRAMP Ready status may minimize the initial security assessment, but will not impact any fees MIS requires.