



FEDRAMP HIGH (CLASS D) CERTIFIED CLOUD PLATFORM

FISMA-COMPLIANT DRUPAL HOSTING

Operating Drupal in a Fully Managed, Federal Security-Compliant Environment

2026 EDITION • **FEDRAMP HIGH PAAS** • **NIST 800-53 REV 5** • **FISMA**

INSIDE THIS GUIDE

The compliance challenge • Platform architecture • Automated Drupal management • Supported Drupal versions • Continuous monitoring • Shared-responsibility model • Documentation bundle & migration

FOR

Drupal Administrators • Federal Site Owners • Government Contractors

GovDataHosting

FedRAMP High (Class D) Certified • DoD IL2 Authorized • U.S. Cloud Data Centers Only

www.govdatahosting.com | 800-967-1004

What's Inside

01 Understanding Your Compliance Challenge

Why FISMA infrastructure is a different problem from Drupal administration

02 Platform Architecture

How each layer implements the NIST 800-53 High baseline

03 Automated Drupal Management

Core patching, maintenance windows, and supported Drupal versions

04 Continuous Security & Compliance Monitoring

24/7 SOC operations, scanning services, and log retention

05 Your Day-to-Day Responsibilities

The shared-responsibility split between you and our platform

06 Documentation Bundle & Migration

Inherited controls, SSP artifacts, and upgrade assistance

Understanding Your Compliance Challenge

Federal agencies require websites and applications to be hosted on infrastructure that meets strict NIST 800-53 security controls. As a Drupal administrator, you are likely fluent in CMS management — but implementing and documenting the hundreds of security controls required for FISMA authorization is a fundamentally different challenge from running a Drupal site.

This guide explains how our **FedRAMP High (Class D) Certified** platform handles the complex security infrastructure beneath Drupal — so your team can focus on what it does best: managing your site’s configuration, content, themes, and modules.

Traditional DIY Approach vs. GovDataHosting

TRADITIONAL DIY APPROACH	GOVDATAHOSTING MANAGED PLATFORM
Configure cloud servers and networking	Pre-configured, hardened servers
Implement DISA STIG hardening	DISA STIG compliance included
Deploy and maintain Drupal core	Drupal core automatically deployed
Write security documentation	Complete SSP documentation
Manage patching schedules	Automated patching handled
Run vulnerability scans	Continuous vulnerability scanning
Coordinate the ATO process alone	ATO support & inherited controls

Platform Architecture: Built for Federal Compliance

Our infrastructure is designed from the ground up to meet federal security requirements. Every layer — from physical data centers to application hosting — implements NIST 800-53 High baseline controls, so your Drupal site inherits a hardened, audited foundation.

FedRAMP High Cloud U.S.-based government community cloud with geographic redundancy, certified to the NIST 800-53 High baseline.	DISA STIG Hardened Security Technical Implementation Guide configuration applied across all systems.	DDoS / WAF Protection Perimeter defense blocks attacks before they reach your site.
FIPS 140-2 / 140-3 Encryption Validated cryptographic modules protect data at rest and in transit.	Multi-Factor VPN Secure privileged access with OTP or PIV-card authentication.	Automated DR 4-hour RTO/RPO with geographically separate failover.

CONTROL INHERITANCE

Because the platform is FedRAMP High (Class D) Certified, your Drupal system inherits **300+ infrastructure and platform security controls** — dramatically reducing the controls you must implement and document yourself.

Automated Drupal Management

Focus on your Drupal content and configuration while we handle the infrastructure complexity. Our platform automates the tedious security maintenance that typically consumes administrator time — including cloud platform patches, server and operating-system patches, Apache, PHP, and database patches, and Drupal core patches.

Automated Drupal Core Installation & Patching

When Drupal releases security updates, our cloud platform team tests and deploys patches to your environment — typically within 48 hours of release. You receive advance notification of maintenance windows, and rollback procedures are in place if any issue arises.

Supported Drupal Versions

VERSION	STATUS	SUPPORT LEVEL	END OF LIFE
Drupal 12	Releasing Dec 2026	Planned support on release	Projected ~2030
Drupal 11	Current / Recommended	Full support	December 2028 (projected)
Drupal 10	Supported	Plan migration to Drupal 11	December 9, 2026
Drupal 9	End of Life	Migration required	November 2023
Drupal 8	End of Life	Migration required	November 2021
Drupal 7	End of Life	Migration required	January 2025

IMPORTANT: END-OF-LIFE VERSIONS

Sites running end-of-life Drupal versions no longer receive security patches and will accumulate high- and moderate-severity vulnerabilities. They may not meet FISMA ATO or continuous-monitoring requirements. We offer migration assistance to help you upgrade efficiently — note that Drupal 10 reaches end of life on December 9, 2026, alongside the Drupal 12 release.

Continuous Security & Compliance Monitoring

FISMA requires continuous monitoring — not just an initial authorization. Our platform includes comprehensive scanning and monitoring services operated by our in-house, U.S.-based Security Operations Center (SOC) in Columbia, Maryland, staffed by U.S. citizens.

Automated Scanning Services

- **Infrastructure Vulnerability Scanning** — cloud infrastructure scans of containers, servers, network devices, and operating systems
- **Drupal Application Scanning** — continuous monitoring for CMS vulnerabilities and outdated modules
- **Section 508 Accessibility Scanning** — automated accessibility-compliance checks
- **External Web Application Scanning** — identifies potential vulnerabilities in publicly reachable web application surfaces
- **Security Log Monitoring** — 24/7 SOC monitoring with extended audit-log retention (12 months active plus 18 months archived), aligned to current federal event-logging requirements

CONTINUOUS MONITORING (COMMON)

Our SOC performs ongoing continuous monitoring — vulnerability scanning, alerting, POA&M management, and monthly compliance reporting — so your authorization stays current between assessment cycles.

Your Day-to-Day Responsibilities

With infrastructure and platform security handled by our team, you can concentrate on the work that delivers value to your mission. This shared-responsibility model defines exactly what you manage and what we manage.

YOU MANAGE	WE MANAGE
• Drupal site configuration	• Cloud server / container configuration & hardening
• Content creation & management	• Cloud network, WAF & firewall management
• Theme customization	• Drupal core installation and patching
• Custom module development	• Database administration
• Contributed module selection	• Backup & disaster recovery
• User roles & permissions	• Security monitoring & compliance
• Section 508 content compliance	• Audit coordination & artifact collection

INFRASTRUCTURE VS. APPLICATION CONTROLS

GovDataHosting guarantees the infrastructure and platform controls; you remain responsible for application-layer controls — your Drupal configuration, content, custom code, and the data you place in the system.

Documentation Bundle & Migration

Our optional managed bundle includes the security documentation required for your FISMA authorization. Because you inherit a significant share of controls from the platform's FedRAMP High (Class D) certification, your documentation burden is dramatically reduced.

Included Documentation

- **System Security Plan (SSP) templates** — pre-populated with inherited platform controls
- **Control inheritance documentation** — clear mapping of platform vs. application responsibilities
- **Continuous monitoring reports** — monthly ConMon artifacts for your authorizing official
- **Incident response procedures** — aligned to federal reporting requirements
- **Annual assessment support** — evidence collection and audit coordination

NEED DRUPAL HOSTING OR MIGRATION ASSISTANCE?

Whether you are starting a new Drupal site or running an end-of-life version, our team can plan and execute a migration to a supported release while maintaining compliance. Migration services include:

Current-environment assessment and upgrade-path analysis • module compatibility evaluation and alternatives • data migration and content preservation • a testing environment for validation before production cutover.

Call 800-967-1004 or visit www.govdatahosting.com to get started.

Next Steps with GovDataHosting

Move your Drupal site onto a federal security-compliant platform and let our team carry the infrastructure, security, and compliance load.

Why GovDataHosting for Drupal

- **FedRAMP High (Class D) Certified platform:** a hardened, audited foundation built to the NIST 800-53 High baseline
- **Control inheritance:** 300+ infrastructure and platform controls inherited — you document only your application-layer controls
- **Automated Drupal management:** core installation and patching, typically within 48 hours of a security release
- **24/7 U.S.-based SOC:** continuous monitoring — vulnerability scanning, POA&M management, and monthly ConMon reporting — staffed by U.S. citizens
- **U.S. data residency:** U.S. cloud data centers only, with U.S.-citizen support staff
- **Migration support:** structured upgrade paths from end-of-life Drupal versions while maintaining compliance

READY TO SIMPLIFY FISMA COMPLIANCE FOR YOUR DRUPAL SITE?

Request a demo or speak with our federal compliance team today.

800-967-1004

www.govdatahosting.com • info@govdatahosting.com

Available on GSA MAS • Maryland CATS+ • NGITS • DoD ACCENT



A Division of IT-CNP, Inc. • Founded 2001

FedRAMP High (Class D) Certified • DoD IL2 Authorized • NIST 800-53 Rev 5 High • SOC 2 Type II

© 2026 IT-CNP, Inc. All rights reserved.

DISCLAIMER

The information in this guide is accurate as of the date of publication. Drupal version lifecycles and end-of-life dates, federal security requirements — including NIST 800-53 guidance, FISMA and FedRAMP policy, Section 508 standards, and federal event-logging requirements (OMB M-21-31, as updated by OMB M-26-14 in 2026) — evolve over time and are subject to change. This guidance can change rapidly. Always verify the latest information at authoritative sources such as drupal.org, fedramp.gov, and nist.gov before making compliance decisions.