GOVDATAHOSTING
POWERED BY IT-CNP, INC.

FEDRAMP HIGH (CLASS D) CERTIFIED CLOUD PLATFORM

FISMA COMPLIANCE FOR FEDERAL RESEARCH GRANTS

A Practical Guide to Budgeting, Building & Maintaining Compliance for Federally Funded Research

2026 EDITION · FISMA · NIST 800-53 · FIPS 199

INSIDE THIS GUIDE

Does your grant require FISMA? • FIPS 199 impact levels • Budgeting compliance • Timeline & the 30-day add-on • Control inheritance • Procurement vehicles • Pre-award checklist

FOR

Principal Investigators • Grant Writers • Sponsored-Programs & Research-Computing Teams

GovDataHosting is a Division of IT-CNP, Inc.

FEDRAMP HIGH (CLASS D) CERTIFIED · NIST 800-53 REV 5 HIGH · DoD IL2 AUTHORIZED

www.govdatahosting.com 800-967-1004

What's Inside

Federal sponsors increasingly attach information-security obligations — FISMA, NIST 800-53, FedRAMP, and Controlled Unclassified Information — to the research they fund. This guide helps principal investigators, grant writers, and sponsored-programs teams recognize when FISMA applies, categorize a system correctly, budget compliance into a proposal, and inherit hundreds of controls from a FedRAMP High (Class D) Certified platform rather than build them from scratch.

1 **Does Your Grant Require FISMA?**
How to spot FISMA, NIST, and CUI obligations hidden in your funding opportunity and award terms

2 **Understanding FIPS 199 Impact Levels**
Categorizing your system Low, Moderate, or High — and why the high-water mark drives your budget

3 **Budgeting FISMA Into Your Proposal**
The direct-cost line items to include, mapped to the companion Grant Budget Template

4 **Timeline & the 30-Day Compliance Add-On**
What compliance really adds to your schedule when you start from a pre-authorized platform

5 **NIST 800-53 Control Inheritance**
How a FedRAMP High (Class D) Certified platform lets your project inherit 300+ controls

6 **Procurement Vehicles for Universities**
GSA MAS, HHS BPA, Maryland CATS+, and sole-source paths to bring the platform onto your award

7 **Pre-Award Compliance Checklist**
A ten-point checklist and a plain-English glossary to act on before your next submission

WHAT YOU'LL FIND INSIDE

Seven short sections take you from "does this even apply to me?" through a pre-award checklist you can act on before your next submission. A companion Grant Budget Template (Microsoft Excel) mirrors the cost categories in Section 3 so you can drop realistic, defensible numbers straight into your budget justification.

01

Does Your Grant Require FISMA?

The Federal Information Security Modernization Act (FISMA) requires federal agencies — and the organizations that operate information systems on their behalf — to protect the confidentiality, integrity, and availability of federal data. For a research institution, the trigger is simple to state: if your project collects, stores, transmits, or processes data on behalf of a federal agency, FISMA very likely applies to the system that handles it.

The obligation rarely arrives with the word "FISMA" in bold. It hides in the security and data-management language of the funding opportunity and the award terms. Read those documents with a security lens and look for the signals below.

WHERE TO LOOK	WHAT SIGNALS A FISMA OBLIGATION
Funding opportunity (NOFO / RFP / RFA)	References to FISMA, NIST SP 800-53, FedRAMP, NIST SP 800-171, CMMC, or "adequate security" for federal data.
Award terms & conditions	Requirements for an Authority to Operate (ATO), a System Security Plan (SSP), continuous monitoring, or agency security review before data is handled.
Data use / data management plan	Handling of PII, PHI, human-subjects data, or Controlled Unclassified Information (CUI) originating from or destined for a federal agency.
Agency security handbooks	Agency-specific mandates such as VA Handbook 6500, HHS/NIH data-security policy, or DOE cybersecurity directives incorporated by reference.

Which Sponsors Most Often Impose It

Requirements are most common on awards from agencies that routinely fund work with sensitive data: NIH and HHS (biomedical and clinical data), the VA (veteran health records), DOE (research databases and national-lab collaborations), NSF (secure research infrastructure), and NASA (mission and research data). The same award can carry overlapping obligations — FISMA for federal security, HIPAA for health data, and FERPA for student records — which a single compliant environment can satisfy together.

NOT SURE WHETHER IT APPLIES? ASK FIRST.

If the language is ambiguous, don't guess — and don't wait until after the award. The GovDataHosting Compliance Team will review your funding opportunity and draft award terms at no cost and tell you whether FISMA applies, at what impact level, and what it means for your budget. Call 800-967-1004.

02

Understanding FIPS 199 Impact Levels

Once you know FISMA applies, the next question is how much security is enough. FIPS 199 answers it by categorizing a system's impact as Low, Moderate, or High across three security objectives — confidentiality, integrity, and availability — based on the harm that a breach of each would cause. The system's overall category is set by the highest of the three (the "high-water mark"), and that category drives which NIST 800-53 control baseline you must satisfy.

Getting the categorization right matters for your budget: control counts and assessment effort scale sharply from Low to Moderate to High. Categorize too low and you risk failing agency review; too high and you over-spend scarce grant dollars. The examples below are typical starting points — your agency and IRB may direct otherwise.

EXAMPLE RESEARCH DATA	COMMON CATEGORIZATION	TYPICAL NIST BASELINE
De-identified or publicly releasable datasets	Low	NIST 800-53 Low
Human-subjects PII; identifiable survey data	Moderate	NIST 800-53 Moderate
Protected Health Information (PHI); clinical-trial data	Moderate–High	Moderate or High
CUI or agency-designated sensitive research data	Moderate–High	Moderate or High

THE HIGH-WATER MARK RULE

A system is categorized at the highest impact level of any data it holds. One Moderate dataset pulls an otherwise-Low system up to Moderate. Segmenting genuinely different data into separate systems or enclaves can keep each at the lowest defensible level — an architecture decision worth making before you write the budget, not after.

A Worked Example

Consider a survey system holding identifiable participant contact information. A disclosure would cause moderate harm, so confidentiality is Moderate. The results must be accurate for the study to be valid, so integrity is Moderate. The system can tolerate a short outage without real damage, so availability is Low. Applying the high-water mark, the system is categorized Moderate overall and must meet the NIST 800-53 Moderate baseline — not Low, and not High.

This is also where the shared-responsibility model begins to save money. You categorize and secure your application and your data; the underlying platform already carries the infrastructure controls. Section 5 explains how that inheritance works.

03

Budgeting FISMA Into Your Proposal

FISMA compliance should be designed alongside your study — not retrofitted after the award. Building it in-house or stitching together multiple vendors is expensive and slow; universities frequently report that meeting FISMA requirements adds roughly 35% or more to the technology cost of a system. A managed, pre-authorized platform converts that unpredictable overhead into a single, defensible line item.

Include the following direct-cost categories in your budget. They map one-for-one to the companion Grant Budget Template so you can enter figures and let it total the period of performance for you.

BUDGET LINE ITEM	WHAT IT COVERS	TYPE
One-time onboarding & setup	Environment provisioning, boundary definition, migration and configuration for the awarded system.	One-time
Hosting & infrastructure	Compute, storage, and network on the FedRAMP High (Class D) Certified platform.	Monthly
IaaS management & administration	Technical staff who configure, monitor, and troubleshoot the computing infrastructure day to day.	Monthly
Bundled compliance services	ISSO support, security engineering, SSP and documentation maintenance.	Monthly
ATO & 3PAO assessment support	Evidence collection, assessment coordination, and agency ATO package support.	One-time / annual
Continuous monitoring (ConMon)	24/7 U.S.-based SOC: scanning, alerting, POA&M management, monthly ConMon reporting.	Monthly

Direct Costs, F&A, and the Period of Performance

Most research grants run three to five years, so budget the recurring items across the full period of performance, not just Year 1. The template carries Year 1–Year 5 columns and a configurable annual escalation so multi-year totals stay consistent.

These are direct costs and are generally subject to your institution's negotiated Facilities & Administrative (F&A / indirect) rate, applied to Modified Total Direct Cost (MTDC). Treatment of cloud and equipment-like costs varies by institution and by sponsor — confirm how your sponsored-programs office classifies managed cloud services before finalizing the budget, because it affects the indirect recovery on these lines.

An Illustrative Multi-Year Snapshot

The figures below show how the categories come together across a three-year period of performance. Every number is illustrative and rounded for planning only — enter your own scoped figures in the companion template.

BUDGET LINE ITEM	ONE-TIME	MONTHLY	3-YEAR SUBTOTAL
Onboarding & setup	$8,000	—	$8,000
Hosting & infrastructure	—	$2,500	$90,000

BUDGET LINE ITEM	ONE-TIME	MONTHLY	3-YEAR SUBTOTAL
IaaS management & administration	—	$1,800	$64,800
Bundled compliance services	—	$2,000	$72,000
ATO & 3PAO assessment support	$12,000	—	$12,000
Continuous monitoring (ConMon)	—	$1,200	$43,200
Estimated 3-year direct total	—	—	≈ $290,000

Illustrative estimates only. Direct costs shown before application of your institution's F&A / indirect rate.

> ⚠ **ILLUSTRATIVE ESTIMATES — NOT A QUOTE**
>
> All dollar figures, percentages, and cost ranges in this guide and the companion template are illustrative estimates for planning only. They are not a quote, a commitment, or financial advice. Actual pricing depends on system scope, impact level, and configuration. Confirm figures with GovDataHosting and validate budget treatment with your sponsored-programs office before submission.

Presented this way, compliance becomes a single, explainable line in your budget justification — something a program officer can evaluate at a glance instead of a scattered set of hardware, software, and personnel costs.

04

Timeline & the 30-Day Compliance Add-On

The fear that security compliance will add a year to a project is usually a fear of doing it from scratch. When you start from a pre-authorized platform and engage early, FISMA compliance typically adds 30–60 days to your timeline — measured against the 12–18 months an institution can spend standing up and assessing an environment on its own.

PHASE	KEY ACTIVITIES	TYPICAL DURATION
Pre-award	Review terms, categorize under FIPS 199, choose baseline, budget line items.	During proposal
Onboarding	Provision environment; basic cloud setup in as little as 1–3 days.	1–3 days
System build	Deploy application, apply inherited controls, document the SSP.	2–4 weeks
ATO package & assessment	Evidence collection, 3PAO / agency assessment, POA&M.	2–6 weeks
Continuous monitoring	Ongoing scanning, monthly ConMon reporting, POA&M management.	Life of award

ENGAGE BEFORE YOU SUBMIT

The single highest-leverage move is to bring the platform provider in during proposal writing. Early engagement lets you cite the right impact level, budget accurately, and reference an existing FedRAMP authorization — often a differentiator in agency review — rather than scrambling to build an environment after the money arrives.

05

NIST 800-53 Control Inheritance

Control inheritance is the mechanism that makes all of the above affordable. Because the GovDataHosting platform is FedRAMP High (Class D) Certified, more than 300 NIST 800-53 Rev 5 controls are already implemented, assessed, and continuously monitored at the infrastructure and platform layers. Your project inherits those controls instead of designing, documenting, and testing them itself.

Inheritance follows a shared-responsibility model. The platform guarantees the controls it owns; your team owns the controls specific to your application, your data, and your organization. A Customer Responsibility Matrix (CRM) documents exactly where the line falls so nothing is assumed and nothing is missed.

CONTROL AREA (EXAMPLES)	WHAT IT INVOLVES	OWNER
Physical & environmental, network boundary	Data-center security, hardened infrastructure, boundary protection.	GovDataHosting
Vulnerability scanning & monitoring	Continuous scanning, alerting, POA&M and ConMon reporting.	GovDataHosting
Configuration & patch management (platform)	Baseline hardening and patching of managed infrastructure.	GovDataHosting
Access control & least privilege (app)	User provisioning, roles, and permissions within your application.	Client
Data classification & handling	Categorizing, labeling, and governing your research data.	Client
Awareness training; incident response plan	Organizational policies and personnel practices for your team.	Shared

FROM THE GOVDATAHOSTING COMPLIANCE TEAM

“Inheritance is the difference between assessing 300-plus controls yourself and inheriting them — so your team can focus on the handful that are truly yours to own.”

WHO WATCHES IT AFTER GO-LIVE

Continuous monitoring is delivered by a 24/7 U.S.-based Security Operations Center staffed by U.S. citizens. The SOC runs vulnerability scanning, alerting, and POA&M management, and produces the monthly ConMon reporting agencies expect — so the authorization you earn at ATO stays healthy for the life of the award without you hiring a security team.

06

Procurement Vehicles for Universities

A FedRAMP-authorized, contract-ready provider is easier to bring onto an award than a bespoke build. GovDataHosting is available through several vehicles, and many institutions can also procure through their own state contracts or a sole-source justification where an existing FedRAMP authorization is a differentiating factor. Your sponsored-programs or procurement office can help identify the cleanest path.

CONTRACT VEHICLE	NOTES
GSA Multiple Award Schedule (MAS)	Broadly available governmentwide vehicle for federal and many federally funded buyers.
HHS BPA	Blanket Purchase Agreement well suited to NIH/HHS-funded research awards.
Maryland CATS+	State vehicle for Maryland institutions and eligible entities.
Institutional / sole-source	Your own state contracts or a sole-source justification citing our FedRAMP authorization.

PROCUREMENT GUIDANCE, NOT LEGAL ADVICE

Contract-vehicle eligibility and sole-source justifications depend on your institution's rules and your sponsor's terms. Treat this as a starting point and confirm the right vehicle with your procurement office and GovDataHosting.

07

Pre-Award Compliance Checklist

Work this list before your next submission. Each item is something you can do now — most of it during proposal writing — to keep compliance from becoming a post-award emergency.

- Review the funding opportunity and draft award terms for FISMA / NIST / CUI language.
- Determine whether your system handles federal data (collect, store, transmit, or process).
- Categorize the system under FIPS 199 and set the impact level using the high-water mark.
- Select the matching NIST 800-53 baseline (Low / Moderate / High).
- Enter direct-cost line items into the Grant Budget Template across the full period of performance.
- Confirm F&A / indirect treatment of managed cloud costs with your sponsored-programs office.
- Request a control-inheritance / CRM review to see which controls you inherit vs. own.
- Reference your platform's FedRAMP authorization and impact level in the proposal narrative.
- Write compliance into the budget justification as a single, defensible line item.
- Plan the ATO timeline so assessment finishes before data handling begins.

Key Terms at a Glance

A quick reference to the acronyms that appear in funding opportunities, award terms, and this guide.

TERM	WHAT IT MEANS
FISMA	Federal Information Security Modernization Act — the law requiring protection of federal information systems.
FIPS 199	The standard for categorizing a system's impact as Low, Moderate, or High.
NIST 800-53	The catalog of security controls; the required set (baseline) scales with impact level.
Baseline	The controls required for a given impact level — Low, Moderate, or High.
ATO	Authority to Operate — an agency's formal approval to run a system with federal data.
SSP	System Security Plan — documents how each control is implemented.
POA&M	Plan of Action & Milestones — tracks and remediates open security findings.
ConMon	Continuous Monitoring — ongoing scanning, alerting, and monthly reporting.
CUI	Controlled Unclassified Information — sensitive federal data requiring safeguarding.
CRM	Customer Responsibility Matrix — documents which controls the platform owns vs. the client.
3PAO	Third Party Assessment Organization — an accredited independent assessor of controls.
FedRAMP	Federal program that standardizes security authorization for cloud services.
F&A / MTDC	Facilities & Administrative (indirect) rate applied to Modified Total Direct Cost.

TERM	WHAT IT MEANS
NOFO / RFA	Notice of Funding Opportunity / Request for Applications — the solicitation.

Ready to Simplify FISMA for Your Research?

Whether you're writing a proposal or already hold an award with security requirements, GovDataHosting will show you exactly how to budget, build, and maintain compliance without disrupting your research — on infrastructure that already carries 300+ inherited NIST 800-53 controls.

REQUEST A GRANT COMPLIANCE REVIEW

Talk to the GovDataHosting Compliance Team about your award:

800-967-1004

govdatahosting.com/education-non-profit-fisma-compliant-cloud-research-grants

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

A Division of IT-CNP, Inc. • Founded 2001 • 800-967-1004 • U.S. Cloud Data Centers Only

DISCLAIMER

This guide is for general planning information only and does not constitute legal, financial, contractual, or compliance advice. All dollar figures, percentages, timelines, and control counts are illustrative estimates for planning only — not a quote or commitment; actual pricing and requirements depend on system scope, impact level, and configuration. FISMA, FIPS 199, NIST 800-53, and FedRAMP requirements evolve over time and vary by sponsor and solicitation. Confirm figures with GovDataHosting and validate compliance and budget treatment with your sponsored-programs office before submission. Authoritative sources include csrc.nist.gov and fedramp.gov.