CASC | Coalition for Academic Scientific Computation

CASC Briefing: Harmonizing Federal Cybersecurity Compliance for Research Data

Background

The Coalition for Academic Scientific Computation (CASC) represents more than 100 U.S. institutions supporting federally funded scientific research. Research Computing and Data (RCD) centers—core to genomics, biomedical, defense, and advanced computing research—are increasingly burdened by fragmented and inconsistent cybersecurity requirements tied to **NIST SP 800-171**.

📄 *Our community has developed a detailed Positions Paper on NIST SP 800-171 compliance (July 2025).*

The Challenge: Fragmentation & Complexity

Research institutions face **conflicting and overlapping requirements** in contracts and data-use agreements from various federal agencies, such as NIH, DoD, NASA, and others, some encoded in Federal Acquisition Regulations (FAR) and supplements (DFARS). Different agencies and contracting contexts may refer to different standards(e.g. NIST 800-53 moderate vs. NIST 800-171), different versions of standards(e.g. NIST 800-171r2 vs. 800-171r3), and add custom requirements. When the requirements flow through subcontracts and collaborative agreements, the resulting collection of requirements becomes unmanageable, adding cost and inefficiencies to the federally funded research ecosystem.

*Without action, these challenges threaten the sustainability of federally funded research, institutional competitiveness, and national security goals***.**

Key Burdens: - **Divergent Standards –** Multiple versions of NIST 800-171 (Rev. 2 vs. Rev. 3) applied simultaneously. - **Lack of Harmonization –** The requirement to meet inconsistent compliance frameworks leads to the need to deploy and operate separate compliance environments (HIPAA, CMMC, NIH), undermining efficiency.

Unsustainable Costs – Duplicative infrastructure and third-party assessments increase costs unnecessarily. - **Rapid Implementation Timelines** – New NIH rules (effective Jan 1, 2025) allow less than a year to retrofit complex computing environments.

A Call for Federal Coordination

CASC urges agencies and coordinating bodies to:

1. **Adopt a Common Standard** – Align on a single, stable version of NIST SP 800-171, with explicitly specified crosswalks and timelines for transitions to new versions.
2. **Standardize Oversight** – Make consistent expectations for POAMs, SSPs, and audit processes explicit in contracts with explicit specification of how requirements flow down to and through subcontracts.
3. **Scale Compliance by Risk** – Following NIST-documented risk-management guidelines, clearly specify when self-attestation is allowed for lower-risk projects and when external audits and external certification are required for high-risk projects.
4. **Support Shared Infrastructure** – Organize, advocate, and support with finding opportunities to build national and regional resource centers to provide environments for research that meet all compliance requirements to serve all institutions large and small throughout the nation.

Next Steps

CASC is committed to working with **federal agencies, Congress, and peer organizations** to create a **consistent, efficient, and equitable compliance framework**. Aligning cybersecurity requirements across agencies will:

- Reduce institutional burden and duplication,
- Enhance research integrity and security, and
- Strengthen the nation’s scientific and innovation enterprise.

Contact:
Coalition for Academic Scientific Computation (CASC)
🌐 https://casc.org