December 26, 2025

Office of Science and Technology Policy
OSTP-TECH-2025-0100

Re: RFI Response: Accelerating the American Scientific Enterprise

Dear Colleague:

The University Corporation for Advanced Internet Development (d/b/a “Internet2”) submits these comments in response to the Office of Science & Technology Policy’s (“OSTP”) Request for Information which seeks input on strategies to “accelerate the American scientific enterprise, enable groundbreaking discoveries, and ensure that scientific progress and technological innovation benefit all Americans.” Internet2 respectfully recommends the following with respect to certain questions posed by OSTP:

(viii): Preparing for AI-Transformed Scientific Research

Advances in AI-assisted scientific research – ranging from automated hypothesis generation and literature synthesis to autonomous experimentation – are poised to accelerate discovery across disciplines. To responsibly realize these capabilities at national scale while preserving scientific rigor and research integrity, the federal government should expand shared AI infrastructure, adopt distributed organizational models, and invest in the cyberinfrastructure workforce. The NAIRR Pilot has demonstrated clear demand for viable public-private collaboration, and the importance of governance, networking, and facilitation models that translate complex AI capabilities into tangible advances in scientific research.

A. Sustained Infrastructure Investments

The federal government should prioritize a national, shared AI research infrastructure that democratizes access for researchers and educators at all institution types, with stable funding and policy frameworks that enable long-term planning.

1. **Expand the NAIRR to full operational status.** The NAIRR Pilot has validated the model of connecting researchers to advanced AI resources through a coordinated, multi-agency and multi-partner platform. The next step is a fully funded NAIRR Operations Center with multi-year appropriations, a service roadmap aligned to community needs, and service-level targets for provisioning, uptime, support, and security. A fully operational NAIRR should include coordinated allocation programs, seamless identity and access management, integrated training pipelines, and mechanisms to onboard new resources as technologies evolve. Formalizing an operations center will also support standardized long-term stability across agencies and partners.

2. **Invest in high-performance research networking.** AI-driven research is increasingly data-intensive and collaborative, generating unprecedented data volumes. Federal investment should increase capacity and resiliency across Internet2's national backbone and regional networks; enabling multi-terabit connectivity and low-latency peering among supercomputing facilities, cloud providers, and research institutions is essential to eliminate bandwidth bottlenecks that throttle AI workflows.

3. **Fund distributed AI infrastructure at regional nodes.** A hub-and-spoke model that locates AI-capable infrastructure at regional network hubs and at minority-serving, rural, and emerging research institutions will broaden participation and reduce latency to users and instruments. Federal programs should support regional GPU/AI accelerators. This distributed approach increases resiliency, builds regional expertise, and ensures that high-impact research and education use cases are not constrained to a handful of national centers.

4. **Support federated, standards-based data infrastructure.** AI for science depends on high-quality datasets that can be securely accessed across institutions. Federal investment should expand federated identity and access management, building on models like Internet2's InCommon federation – which enables researchers to access distributed datasets while maintaining appropriate access controls and provenance tracking.

B. Organizational Models

Organizational structures should ensure that infrastructure investments remain aligned with researcher needs, and maintain rigorous governance and accountability.

5. **Adopt community-driven governance.** The NAIRR should incorporate Internet2's proven governance model in which member institutions, agencies, and community stakeholders collectively set priorities and shape policies. Standing advisory groups should inform allocation policies, acceptable use standards, transparency requirements, and evaluation metrics. Governance should explicitly promote equitable access, openness, and sustainability to align with researcher needs rather than vendor interests.

6. **Strengthen cyberinfrastructure facilitator networks.** Researchers need support to translate AI advances into tangible progress. Federal programs should support the expansion of research computing and data (RCD) professional networks - such as those coordinated by Internet2 and the Campus Research Computing Consortium (CaRCC) - that help researchers effectively use AI tools. These facilitators translate between domain scientists and AI infrastructure, with opportunities to expand region- or state-specific cyberinfrastructure facilitation capacity aligned with nodes of capabilities reflected in regional research and education networks (RENs), and in new regionally-located investments in AI and computing infrastructure.

7. **Formalize public-private partnership frameworks.** The NAIRR Pilot's partnerships with Google, NVIDIA, Microsoft, and others have shown the value of structured partnerships for public research benefit. The federal government should expand these public-private frameworks

for data governance, intellectual property, and sustained access commitments. Agreements should continue to align with federal scientific values.

C. Workforce Development Strategies

Realizing the potential of AI-enabled scientific research requires sustained investment in the people who design, operate, and use these systems, with attention to equity and on-ramps for new communities.

8. Invest in research computing and data (RCD) professional development. The cyberinfrastructure workforce is a critical enabler of AI in science yet remains chronically overlooked in terms of support. Federal initiatives should fund professional development pathways, certifications, and fellowships for RCD professionals, including systems and data engineers, research software engineers, security analysts, and AI platform specialists. CaRCC's workforce development initiatives can be replicated and expanded to meet these objectives.

9. Embed AI literacy across disciplines. Graduate curricula and postdoctoral training should integrate core AI competencies tailored to domain-specific contexts. Scientists need to understand AI's capabilities and limitations to maintain research integrity when using automated tools.

10. Fund hands-on training at scale. Demand for practical AI training far exceeds current capacity. Federal programs should expand support for hands-on workshops, summer institutes, short courses, and curriculum development that leverage NAIRR resources.

D. Maintaining Scientific Rigor and Research Integrity

As AI becomes embedded in the research lifecycle, federal policy should promote safeguards that ensure credible, reproducible, and trustworthy science. To maintain research integrity as AI transforms science, the government should support development of reproducibility frameworks for AI-assisted research, require disclosure and documentation standards for AI methods in federally-funded publications, fund research on AI bias and error detection in scientific applications, and establish community standards for validating AI-generated hypotheses and experimental designs. Together, these investments, organizational practices, and workforce strategies will enable the United States to capture the upside of AI-accelerated discovery while preserving the core values of scientific rigor, openness, and trust.

(xi) Fostering Collaboration Across Scientists, Engineers, and Skilled Technical Workers

Breakthrough research increasingly depends on tight integration of theoretical insight, applied engineering, and sustained operational expertise. Federal policy should explicitly recognize—and invest in—the cyberinfrastructure professionals who translate ideas into scalable research capabilities, and should build shared platforms and training pathways that make collaboration routine rather than exceptional.

A. Recognize and Fund Cyberinfrastructure Professionals.

Research computing professionals, data engineers, scientific software developers, and cyberinfrastructure administrators are the indispensable "connective tissue" between researchers and real-world scientific breakthroughs. Federal grant programs should explicitly allow, and encourage, the direct funding of permanent technical positions as allowable costs, rather than limiting support to short-term project roles.

1. **Allow direct, permanent funding of technical staff.** Federal grants should explicitly allow—and encourage—funding for permanent technical positions as allowable costs, not only short-term project roles. Stable, career-track positions reduce turnover, preserve institutional knowledge, and keep highly skilled personnel in the research ecosystem.

2. **Establish professional career tracks for research computing staff.** Agencies should encourage institutions to create parallel, promotion-eligible pathways for research computing and data professionals, with clear advancement criteria, continuing professional development, and recognition in project deliverables, publications, and grants.

3. **Invest in professional communities.** Sustained support for organizations such as CaRCC and events like PEARC (Practice and Experience in Advanced Research Computing) — communities that Internet2 helps host and support — will disseminate lessons learned, align tools and standards, and strengthen common practices across institutions.

B. Enable Collaborative Infrastructure.

Shared platforms and identity services should lower collaboration barriers while embedding best-practice security, data management, and performance.

4. **Fund shared research platforms.** The federal government should invest in science gateways, virtual research environments, collaborative notebooks, and reproducible workflow systems that create common collaboration testbeds. These platforms lower barriers for scientists while creating natural collaboration points with engineers.

5. **Support identity federation.** Strengthen identity federation infrastructure like InCommon so researchers and technical staff can authenticate across institutions without account sprawl, reducing friction and improving security.

6. **Support cross-institutional, distributed teams.** Create funding mechanisms that support distributed research teams spanning multiple institutions, where theoretical researchers at one institution work with engineering expertise at another. Current funding models often penalize such distributed collaboration.

C. Integrate Training Pathways that Bind Theory to Practice.

Training models should bind theory to practice through sustained, embedded experience rather than transactional consulting arrangements.

7. **Fund apprenticeship models and internships.** Support placements that embed technical staff in research groups—and researchers in operational environments—to build durable relationships and shared understanding. Internet2's engagement model with member campuses demonstrates how sustained relationships between technical and research communities yield better outcomes than transactional consulting.

8. **Create rotation and sabbatical programs.** Enable technical professionals to spend time in active research labs and allow researchers to gain firsthand experience in operational environments. These rotations build mutual understanding and lasting collaborative relationships.

9. **Fund joint and integrated degree programs.** Support graduate training and programs that combine domain science with computational and engineering training. These programs produce researchers equipped to lead interdisciplinary teams.

(xii) Ensuring Federally Funded Research Benefits All Americans

The benefits of federal research — new technologies, high-quality jobs, and improved quality of life — will be maximized when cyberinfrastructure capacity, expertise, and access are purposefully distributed across institutions, regions, and communities. Federal investments should prioritize sustained capacity building, not one-off procurements, and should require meaningful participation by Minority-Serving Institutions (MSIs). Further, the government should leverage national and regional networks to deliver resources where researchers work and students learn.

A. Invest in Minority-Serving Institutions with Sustained Capacity-Building.

Internet2's partnership with the Minority Serving–Cyberinfrastructure Consortium (MS-CC) demonstrates both the need and the path forward. HBCUs, TCUs, HSIs, and other MSIs educate a disproportionate share of underrepresented students in STEM fields but have historically lacked access to the cyberinfrastructure that enables cutting-edge research. To address these imbalances, Internet2 recommends:

1. **Provide sustained infrastructure funding.** The $15 million NSF grant to MS-CC and Internet2 is a start, but MSIs need sustained, multi-year funding for cyberinfrastructure development . The government should focus on multi-year support for cyberinfrastructure staffing, operations, and professional development at MSIs.

2. **Prioritize workforce capacity, not just hardware.** MSIs consistently report that their primary challenge is workforce capacity, not hardware. Federal programs should fund positions for cyberinfrastructure professionals at MSIs, with career development support and connection to national professional networks.

3. **Expand community-of-practice models.** Support MS-CC's on-campus workshops and similar programs that tailor training to institutional context, foster peer support, and create locally sustainable solutions. MSIs consistently report that their primary challenge is workforce capacity. Federal programs should fund positions for cyberinfrastructure professionals at MSIs, with career development support and connection to national professional networks.

4. **Require meaningful MSI participation in major initiatives.** Build MSI inclusion into the design and governance of major federal efforts—including NAIRR—with dedicated resources.

B. Ensure Geographic Equity through Distributed Resources.

5. **Invest in regional research and education networks.** Strengthen state and regional backbones and last-mile connectivity to ensure that rural and smaller institutions can join national collaborations. State and regional research and education networks extend Internet2's reach to every corner of the country. Federal investment in regional network capacity ensures that researchers at institutions in rural areas have the same connectivity as those at major research universities.

6. **Distribute advanced computing resources.** Deploy NAIRR and similar resources across regional nodes to cultivate local expertise, reduce latency, and generate economic benefits in underserved areas.

7. **Align with EPSCoR-style capacity building.** Programs like NSF's EPSCoR (Established Program to Stimulate Competitive Research) demonstrate effective approaches for building research capacity in underserved states. Similar targeted investments in cyberinfrastructure would compound the benefits of EPSCoR investments.

C. Democratize Access to AI and Advanced Computing.

8. **Democratize AI access.** Federal policy should ensure that institutions of all types can effectively access and use national resources. The NAIRR Pilot's mission - democratizing access to AI resources - addresses a critical equity gap. To ensure benefits reach all Americans, the government should make NAIRR allocations available to researchers at any accredited U.S. institution regardless of institutional research ranking, fund cyberinfrastructure facilitation support that helps researchers at under-resourced institutions effectively use national resources, create pathways for community colleges and teaching-focused institutions to access research infrastructure, and develop training materials and support structures accessible to institutions without dedicated research computing staff.

(xiii) Strengthening Research Security While Minimizing Burden

A secure research enterprise is a shared responsibility. Federal policy can both raise the security baseline and reduce compliance burden by investing in shared services, harmonizing and right-sizing requirements, and building a specialized security workforce that understands research environments. Done well, security will enable openness by protecting sensitive work without constraining fundamental research.

A. Invest in Shared Security Infrastructure.

Shared, network-scale capabilities can deliver protection and threat detection that no single institution can achieve alone. Internet2's Trusted Infrastructure Platform and related community programs demonstrate effective models:

1. **Fund network-level security capabilities.** Invest in embedded DDoS mitigation, anomaly detection, and secure peering—such as those in Internet2's Trusted Infrastructure Platform—to lift the baseline for all connected institutions. Federal investment in these shared capabilities provides protection at scale that no individual institution could afford.

2. **Expand routing security programs.** Internet2's Routing Integrity Initiative advances adoption of RPKI, BGP security, and other routing safeguards across the R&E community. Federal support for these programs would strengthen the security foundation for all research traffic.

3. **Strengthen federated identity security.** The InCommon federation provides secure identity infrastructure serving over 16 million users across more than 1,400 institutions. Continued investment in federation security - including support for multi-factor authentication deployment and identity proofing - strengthens the authentication foundation for research access.

4. **Support shared security operations and information sharing.** Support shared security operations centers and information sharing mechanisms - like the REN-ISAC (Research and Education Networking Information Sharing and Analysis Center) - that provide threat intelligence and incident response support to the research community.

B. Develop Proportionate and Harmonized Security Frameworks.

Risk-based, tiered requirements should protect sensitive work without overburdening fundamental research, and should be consistent across agencies.

5. **Adopt risk-based, tiered security controls.** Distinguish fundamental research from sensitive applied work so institutions can apply appropriate controls while preserving openness.

6. **Harmonize agency requirements.** Recognize common frameworks across agencies to reduce duplication and confusion for multi-agency projects.

7. **Provide implementation support.** Fund programs like Trusted CI for hands-on assistance, training, reference architectures, and community toolkits, especially for under-resourced institutions.

8. **Invest in automation and tooling.** Invest in tools and automation that make security compliance easier for researchers. Continuous compliance monitoring, automated reporting, and pre-configured secure research environments reduce the burden on individual researchers while improving actual security outcomes.

C. Build Research-Aware Security Workforce Capacity and Preserve Openness.

Research institutions face a critical shortage of cybersecurity professionals who understand research environments. Federal programs should fund cybersecurity training specifically designed for research computing contexts, support career pathways for research security professionals - including competitive compensation, create fellowship and rotation programs that bring security expertise to under-resourced institutions, and fund security communities of practice - like the MS-CC's Cybersecurity Community of Practice - that enable peer learning and resource sharing.

D. Balance Security and Openness.

The fundamental research enterprise depends on openness, collaboration, and information sharing. Security policies must preserve these values while addressing legitimate risks. Policies should clearly distinguish between fundamental research (which benefits from openness) and sensitive applied research (which may require controls), avoid broad restrictions that chill legitimate international collaboration, recognize that many security risks are better addressed through publication and transparency than through secrecy, and ensure that security compliance costs do not disproportionately burden smaller institutions or discourage their participation in federal research.

CONCLUSION

Taken together, these measures will connect theory and practice through sustained investment in people and platforms; distribute the benefits of research across communities and regions; and raise the security baseline in ways that protect sensitive work without impeding discovery. With intentional design, the same shared infrastructure that accelerates collaboration can also democratize access and improve security, ensuring that federal research investments deliver broad and durable public benefit.

*****

Internet2 appreciates OSTP's consideration of these comments.

Respectfully submitted,

------ /s/ Belinda Nixon
Belinda Nixon
Vice President and General Counsel
Internet2
1150 18th Street, NW
Suite 750
Washington, DC 20036