National AI Research Resource Task Force Final Report

TESS DEBLANC-KNOWLES, SENIOR POLICY ADVISOR,
WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

NAIRR Task Force Objectives

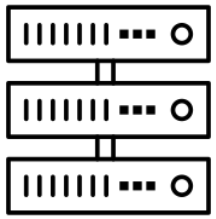
- Investigate the feasibility and advisability of establishing and sustaining a NAIRR
- Propose a roadmap and implementation plan detailing how the resource should be established and sustained

NAIRR Roadmap Elements

i. Goals for the NAIRR
ii. Ownership and administration plan, including responsible agency or organization
iii. Governance and oversight model
iv. Capabilities required
v. Assessment of and solutions to barriers to use of high-quality government data sets
vi. Security requirements and access control framework
vii. Privacy and civil rights and civil liberties requirements
viii. Sustainment plan, including Federal funding and partnerships
ix. Agency roles and responsibilities, implementation milestones, and other key parameters

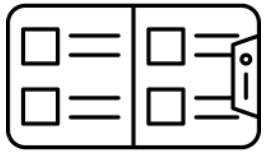
Vision for the NAIRR

A widely-accessible, national cyberinfrastructure that will advance the U.S. AI R&D environment, discovery, and innovation by empowering a diverse set of users through access to:



Secure, high-performance, privacy-preserving **computing**

High-quality **datasets**



Catalogs of **testbeds** and **educational materials**

Training tools and **user support** mechanisms

NAIRR Objective and Goals

Objective: To strengthen and democratize the U.S. AI Innovation ecosystem in a way that protects privacy, civil rights, and civil liberties

Goals:

Spur **innovation**

Increase the **diversity** of talent in AI

Improve U.S. **capacity** for AI R&D

Advance **trustworthy AI**

NAIRR Users

Researchers, **educators**, and **students** at U.S.-based:

- Academic institutions
- Non-profit organizations
- Federal agencies or federally-funded research and development centers (FFRDCs)
- State, local, or tribal agencies
- Startups or small businesses with SBIR, STTR, or similar Federal grants

Federal Administration of NAIRR

Administrative home agency:

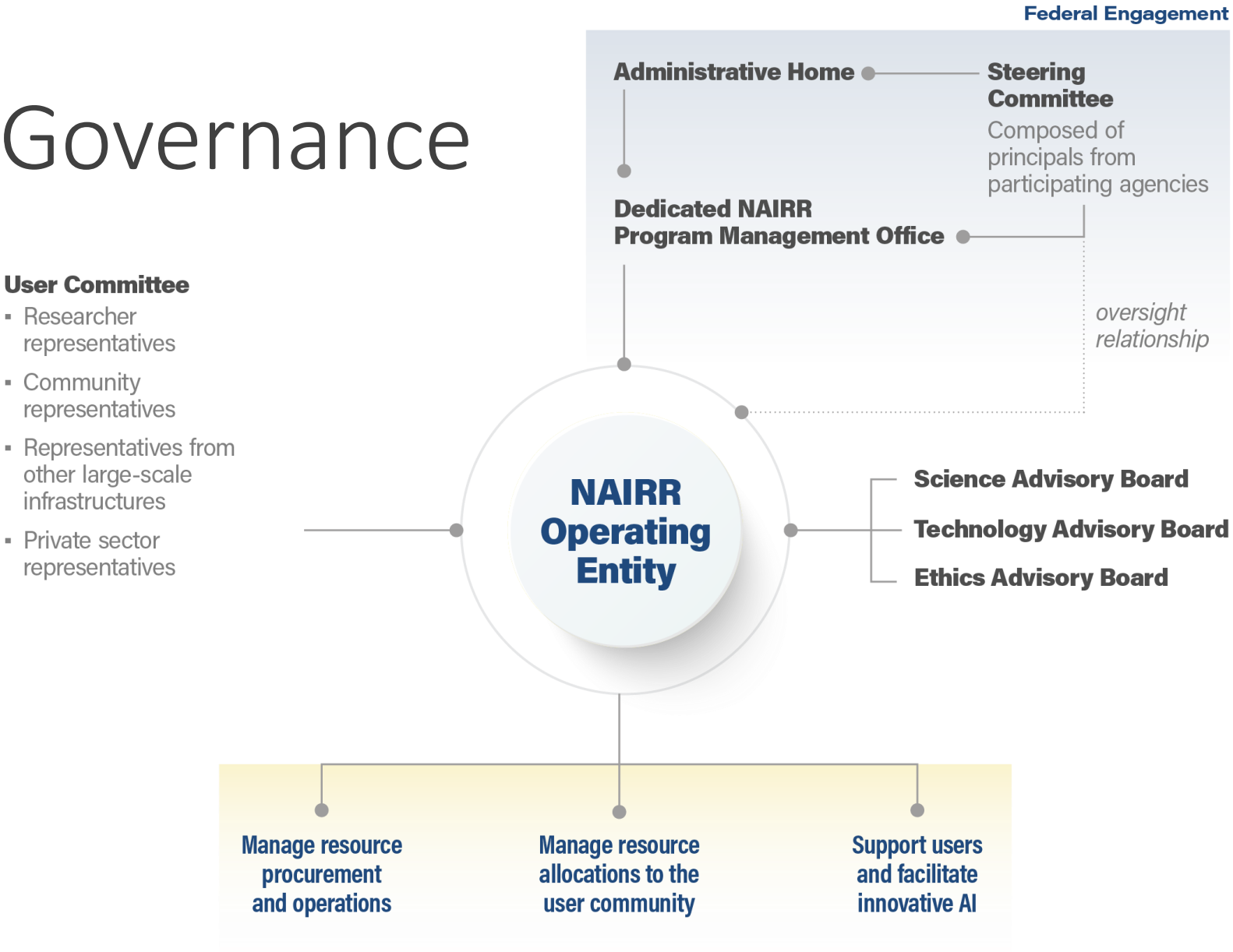
- Mission-aligned with NAIRR
- Existing relationship with AI R&D community
- Experience supporting AI R&D
- Focused on equity and diversity
- Capable of support democratized access
- Funds Operating Entity

Other agencies:

- Serve on Steering Committee
- Fund NAIRR resource providers
- Help staff Program Management Office

By majority opinion, the Task Force recommends that the National Science Foundation serve as the NAIRR's administrative home

NAIRR Governance



NAIRR Composition

- Federation of new and existing resources
- Primarily owned by third-party providers
- Integrated user support and trainings
- Catalogs of data sets, testbeds, and educational resources
- Transparent specifications, policies, and practices
- Secure, robust, accessible, and sustainable
- Integrated access portal

Resource Allocation

NAIRR resources allocated to users via three tracks:

1. **Agency-driven** – *each agency awards a share of credits*
2. **Peer review** – *Operating Entity-managed merit review*
   - Project startup (OE staff)
   - Larger-scale (OE-coordinated panel)
3. **Operating Entity discretionary** – *executive leadership share of credits*

Security and Access Controls

System Design

- Five-safes framework
- Authentication required for all but nominal resources
- Tiered model
  - **NAIRR-Open**: Open science zone
  - **NAIRR-Secure**: Secure enclave(s)
  - Other tiers as necessary

Management

- Expert technical security staff
- Routine monitoring and updates

Governance

- Advisory boards
- User agreements
- Required security and ethics trainings

Privacy, Civil Rights, and Civil Liberties

NAIRR should be an exemplar for transparent, ethical, and responsible AI R&D

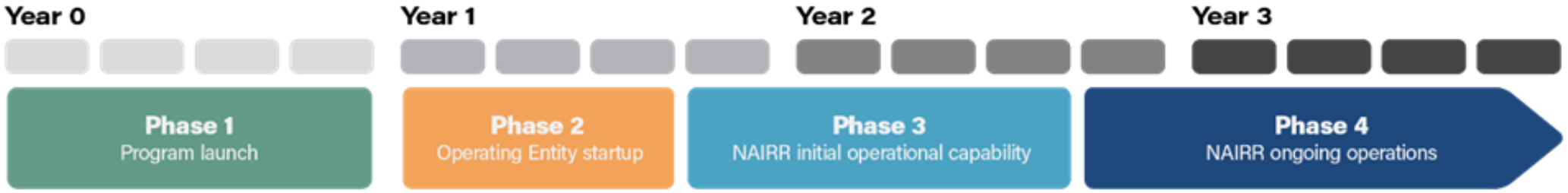
- Transparency and oversight across all aspects
- Guidance from Ethics Advisory Board and User Committee
- Diversity and expertise among decision-makers and staff

Privacy, Civil Rights, and Civil Liberties

The NAIRR Operating Entity should:

- Develop and Publish:
  - Resource acceptance criteria and controls
  - Ethics review criteria and mechanisms
- Draw from:
  - *Blueprint for an AI Bill of Rights*
  - *AI Risk Management Framework*
- Provide data to facilitate R&D on implications of bias
- Ensure annual user and staff training on practices and responsibilities

Phased NAIRR Buildout



Phase 1

- Appropriations
- Establish Program Management Office
- Select Operating Entity

Phase 2

- Fund Operating Entity
- Develop resource provider solicitations
- Establish boards and committees

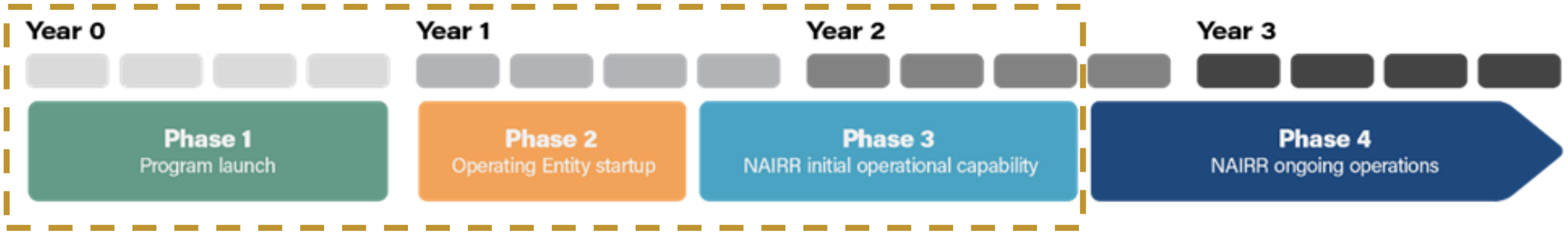
Phase 3

- Allocate resources
- Provide user support
- Collect metrics for evaluation

Phase 4

- Solicit new resource providers
- Support emerging areas of interest
- Participate in evaluation

Optional Pilot



- The Program Management Office could expand access to existing cyberinfrastructure for AI researchers
- This would require:
  - Supplemental funds to existing resource providers beginning in Year 0
  - Interim management and governance mechanisms
- Pilot would operate until the NAIRR is fully operational in Year 2

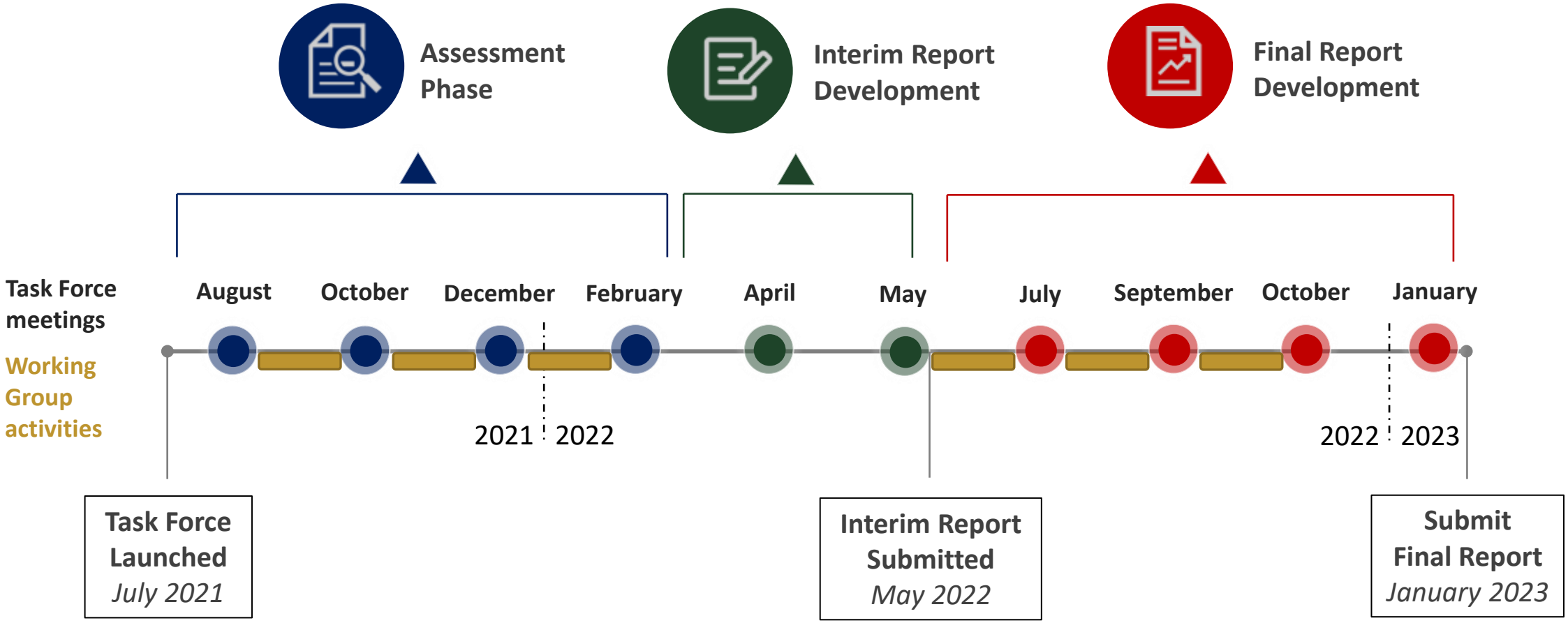
Preliminary NAIRR Budget

Year	Resource Providers	Operating Entity	Evaluation	Total
1	$375M	$70M	$5M	$450M
2	$375M	$60M	$5M	$440M
3	$375M	$60M	$5M	$440M
4	$375M	$60M	$5M	$440M
5	$375M	$60M	$5M	$440M
6	$375M	$60M	$5M	$440M
6-year total	$2.25B	$370M	$30M	~ $2.6B

Final Report Roll Out Plans

MANISH PARASHAR, OFFICE DIRECTOR, OFFICE OF ADVANCED CYBERINFRASTRUCTURE, NATIONAL SCIENCE FOUNDATION

Task Force Timeline and Work Plan



Final Report Release

1. Report Posted to AI.gov

2. Blog Post

3. Public Event

Socialization of Findings & Recommendations

- Briefings to Congress
- Engagement with stakeholders
- Media call
- Social media
- Task Force member networks
- Interagency briefings