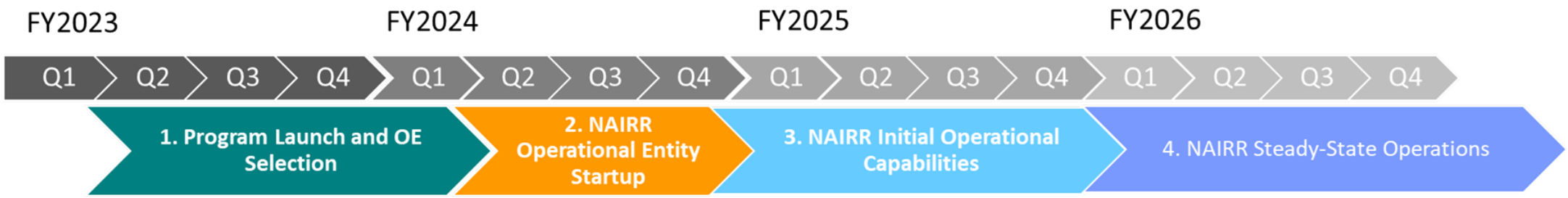
NAIRR STAND UP TIMELINE

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

NAIRR Stand Up Timeline



NAIRR Pilot Option

- Goal: Leverage existing resources, software stacks and user portals, and service providers from the current national cyberinfrastructure ecosystem (with supplemental funding) to deploy a pilot to provide limited resources to the AI R&D community until the NAIRR is fully operational.
  - Assumes rapid establishment of a PMO along with a SC as precursors to the eventual PMO and SC.
  - Initial (albeit limited) allocations by Q4 for FY 2023.
  - Transition to full NAIRR operations in fiscal year 2024.

NAIRR Pilot Option

- Possible timeline:
  - FY23 Q2: Identify relevant service provider and resource providers; develop mechanism for supplementing service and resources providers; issue call for supplements (e.g., a DCL).
  - FY23 Q3: Fund supplements; service and resource providers ramp up and prepare for pilot operations.
  - FY23 Q4: Pilot NAIRR operations with MVP; issues first (limited) call for allocations to the AI R&D community.
  - FY24 Q2: Pilot NAIRR deployment ramps up with addition capacity (staff, resources) at the service and resource providers; initial allocations made to researchers.
  - FY24 Q3 – FY25 Q2: Pilot NAIRR operations with regular call for allocations.
  - FY25 Q3: Pilot NAIRR ramps down and transitions to the full NAIRR deployment.

NAIRR Security moderated discussion

<u>Moderators</u>

Mike Norman

Dan Stanzione

Elham Tabassi

Potential discussion items

- Role of NAIRR-Secure
- NAIRR-Secure enhancements
- NAIRR-Secure security levels
- Usability-security tradeoffs

Role of NAIRR-Secure

- NAIRR-Secure would be a specialized RP assisting individual users and project teams to operate securely in the cloud
  - Compliance is a shared responsibility between cloud provider (“security of the cloud”) and user (“security in the cloud”)
- NAIRR-Secure RP(s) responsibilities include
  - Identity management
  - Onboarding
  - Security awareness training
  - Compliance management and auditing
  - Solution consulting (applications)
  - Security patching (ongoing)

NAIRR-Secure enhancements

- ADRF as reference architecture (ADRF – Coleridge Initiative)
- Multi-cloud
  - Provide more choice and capabilities than single cloud
  - User familiarity
  - Avoid vendor lock-in
- Enable secure data transfers in from secure data sources (e.g. NIH portals) with Inherited access permissions
- Sandboxing (agile prototyping)

NAIRR-Secure security levels

- Interim Report says tiered security levels without specifying what and how many
- Draft final report implies a single security level (beside Open) without specifying it
- Do we need to revisit tiered security? If so, what are the levels and how to implement them?
- ACDEB Governance report recommends three levels public, protected, and restricted
- Alternatively, a single security level like FISMA moderate or CUI level 3 covers most use cases; higher classification levels would likely be done “in agency”

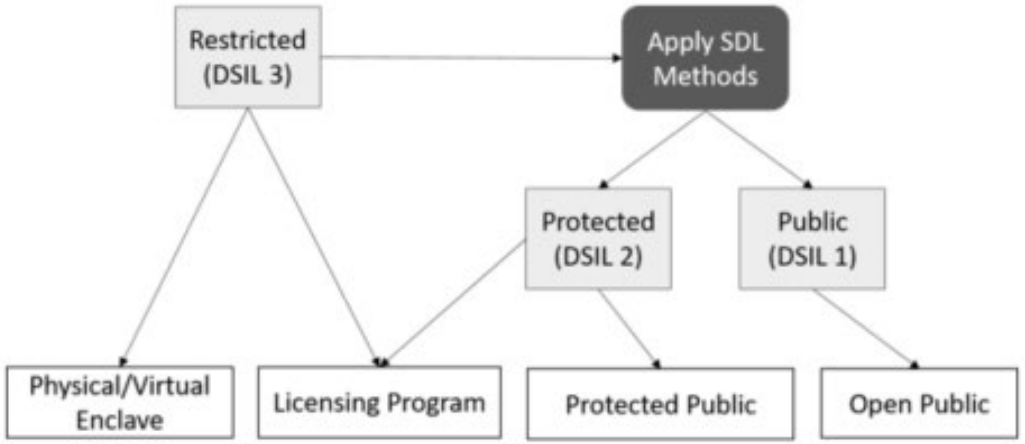


Figure 2. Single data source, multiple paths to access the data or cleaned output.

Advisory Committee on Data for Evidence Building (ACDEB) Governance Report 8/14/2022

Usability-security tradeoffs

- If data is too tightly controlled, it may never be used, hindering access goals
- There is thus a tradeoff between security and usability
- One approach to finding a sensible compromise is to take a risk-based approach to data management, possibly involving tiered access levels and distribution modes (ACDEB Report)

Discussion

NAIRR DATA RESOURCES

JULIA LANE
DANIELA BRAGA

Key points of clarification for moderated discussion

AI repositories where the data is valuable, easily accessed and "ready to ingest“
- How does the NAIRR measure value?
- What do we mean by ready to ingest (searchable, discoverable, documented)?

A role of the NAIRR is to identify data sharing incentives
- Data marketplace
- Search and discovery
- Also applies to models, code, and tools

Role of interaction with Data.gov
- NAIRR will work with data.gov to enhance discoverability of data

National Secure Data Service and government data
- Evolve in parallel
- Complement NSDS in terms of providing access to secure data not in NSDS
- Be informed by approaches to different privacy levels and tiered access

Data resources for initial NAIRR operations – from research projects; public datasets
- Examples: Google: Marketplace – Google Cloud console; Amazon – https://aws.amazon.com/opendata/; Azure Open Datasets | Microsoft Learn; NIH – https://www.nlm.nih.gov/NIHbmic/generalist_repositories.html

NAIRR ADMINISTRATIVE HOME

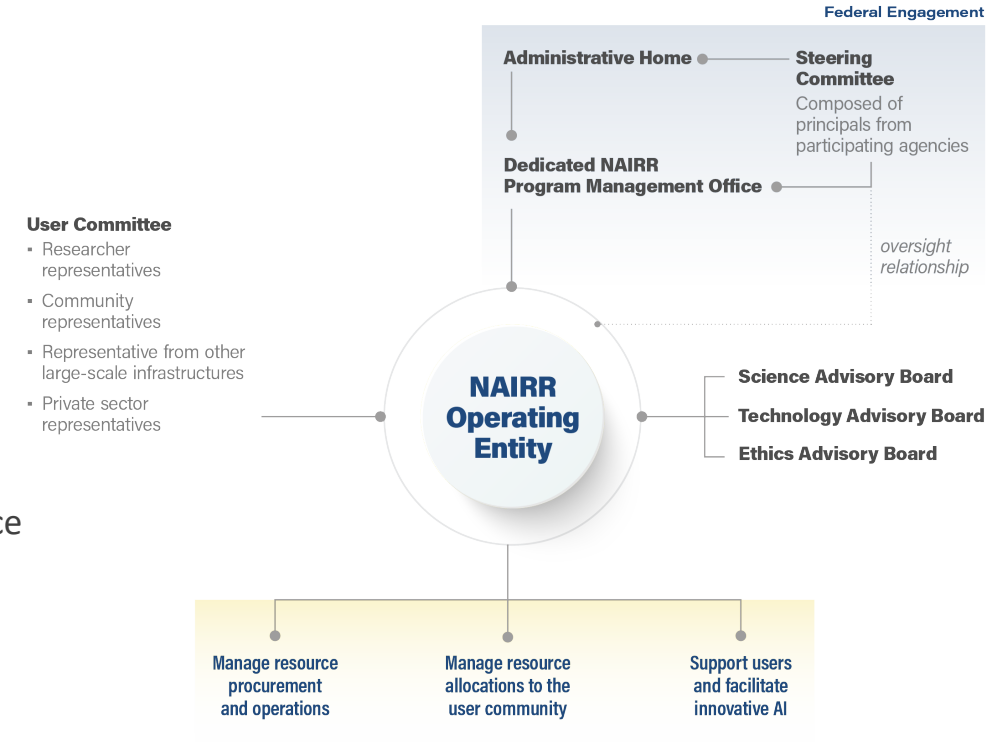
TESS DEBLANC-KNOWLES, SENIOR POLICY ADVISOR, NATIONAL AI INITIATIVE OFFICE,
WHITE HOUSE OFFICE OF SCIENCE AND TECHNOLOGY POLICY

NAIRR Administrative Home & Steering Committee

- Task Force Findings:
  - Designating a single agency to manage the NAIRR would risk narrowing its focus.
  - Having multiple agencies manage and fund the NAIRR raises other potential challenges, such as:
    - A lack of clarity in terms of who is responsible for supporting key components
    - The need for multiple Congressional appropriations committees to coordinate on how to appropriate funds.
- Recommended Approach:
  - A single agency serves as the “operational administrative home” for the NAIRR, providing funding for a third-party Operating Entity that is responsible for the operations of the NAIRR
  - Other agencies actively involved in NAIRR stewardship and oversight by:
    1) Forming a Steering Committee that provides strategic guidance and collective performance evaluation of the NAIRR through the administrative home
    2) Provisioning resources through individual-agency funding for the various resource providers that would be federated together to constitute the NAIRR

NAIRR Administrative Home & Steering Committee

- Operational administrative home responsibilities:
  - Stand up & support a program management office
  - Fund the NAIRR Operating Entity
- Steering Committee responsibilities:
  - Assist in writing and releasing a request for proposals to solicit bids for the NAIRR Operating Entity, including establishing the terms and conditions and functions of the Operating Entity;
  - Work with the NAIRR Program Management Office to review candidates and select the Operating Entity awardee;
  - Identify resources that could be federated, participate in resource provider selection, and provide direction to the Operating Entity about resource allocation and how those resources should be made accessible via the NAIRR;
  - Once the NAIRR has been initiated, define the NAIRR key performance indicators (KPIs); and
  - Evaluate NAIRR performance against the defined KPIs.



Key Characteristics of a NAIRR Administrative Home

- Mission alignment
- Capacity and capabilities to effectively support administrative activities
- Existing relationship with the AI research community and other NAIRR stakeholders
- Experience supporting foundational, use-inspired and translational AI research
- Focus on equity and diversity and ability to support democratization of resource access
- Flexibility in managing interagency agreements

Final Report Development: Key Dates

October 21:	*TF meeting* – deliberate on report content
October 24:	TF written feedback on second draft due
November 4:	Third draft shared with OSTP/NSF leadership
November 30:	Final draft sent to TF
December 7:	*TF meeting* – vote on final report

Per its legislative mandate, the TF will exist for 90 days following submission of the final report. The TF will use December 2022-February 2023 to socialize the recommendations put forth in the final roadmap and implementation plan.