Response of The MITRE Corporation to the OSTP RFI on Implementing Initial Findings and Recommendations of the National Artificial Intelligence Research Resource Task Force

June 30, 2022

For additional information about this response, please contact:
Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

<<This page is intentionally blank.>>

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate six federally funded research and development centers (FFRDCs) that are leveraged by numerous federal agencies, participate in public-private partnerships (PPPs) across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's 9,000-plus employees solve problems for a safer world, with scientific integrity as our foundation. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision-making, technical findings, or policy recommendations.

Over the decades, MITRE has established and supported dozens of interdisciplinary, systems-level partnerships—such as collaboratives, consortia, and specialized PPPs—to bring whole-of-nation focus to achieving national priorities. Examples include the Aviation Safety Information Analysis and Sharing (ASIAS), the Medical Device Information Analysis and Sharing (MDIAS), and the Partnership for Analytics Research in Traffic Safety (PARTS). Because of our close relationships with federal agencies and our prohibition on competing with industry, we often serve these partnerships as a convener, building relationships among historically siloed groups, and as an independent steward of partners' proprietary/sensitive data—given that all parties can trust us to act in a conflict-free manner and focus solely on achieving national public interest objectives. Within ADAS, for example, MITRE supported the partnership by managing, safeguarding, and analyzing data on 47 million vehicles and 12 million crashes, to deliver results about the real-world effectiveness of ADAS. These insights allow partners to make data-driven decisions about enhancements to and investments in advanced driver assistance systems, fostering the safety of US persons traveling by automobile.[1]

MITRE has a 50-year history of partnering with federal agencies to apply the best elements of artificial intelligence (AI) and machine learning (ML) while developing and supporting ethical guardrails to protect people and their personal data. Our team's experience with the entirety of the AI/ML adoption and life cycle has strengthened our ability to anticipate and solve future needs that are vital to the safety, well-being, and success of the public and the country. MITRE has deep expertise in systems engineering and integration, having developed architectures for numerous data sharing and analytics platforms. This includes portals, advanced visualizations, and the necessary security controls to enable shared resources. MITRE has earned the reputation and trust of government, industry, and academia as an honest broker, and we stand ready to serve the interests of the Task Force and the needs of the National Artificial Intelligence Research Resource (NAIRR).

Questions Posed in the RFI

a. Vision for the NAIRR. (Chapter 2 of the report)

MITRE recommends that the approach and substance of current NAIRR vision, goals, composition, etc. be strengthened and clarified. Critically, MITRE recommends NAIRR do that through a collaborative approach to strategic planning with the entities that are most likely to be affected by or involved in NAIRR. Based on prior partnerships, MITRE has found that using approaches that engage potential

[1] Partnership for Analytics Research in Traffic Safety. 2022. NHTSA, https://www.nhtsa.gov/parts-partnership-for-analytics-research-in-traffic-safety. Last accessed June 29, 2022.

partners and end users and allow them to co-design goals and other foundational aspects of their collaboration and associated partnership operating model is a leading indicator of the eventual success of such partnerships.[2] To that end, we recommend NAIRR, together with the relevant stakeholders, use a strategic planning framework consistent with the Government Performance and Results Act to strengthen and clarify the NAIRR concept (see Figure 1).

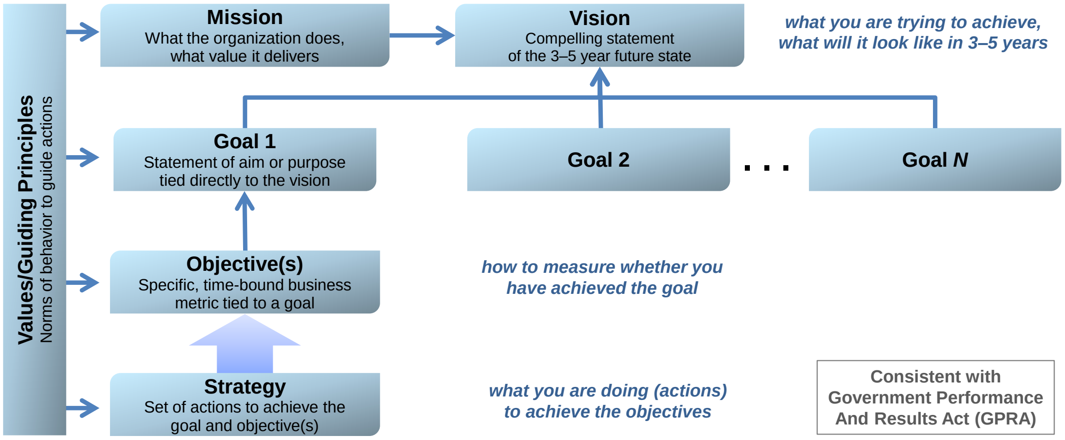
Values/Guiding Principles
Norms of behavior to guide actions
Mission
What the organization does, what value it delivers
Vision
Compelling statement of the 3–5 year future state
what you are trying to achieve, what will it look like in 3–5 years
Goal 1
Statement of aim or purpose tied directly to the vision
Goal 2
. . .
Goal N
Objective(s)
Specific, time-bound business metric tied to a goal
how to measure whether you have achieved the goal
Strategy
Set of actions to achieve the goal and objective(s)
what you are doing (actions) to achieve the objectives
Consistent with Government Performance And Results Act (GPRA)

Figure 1 – Strategic Planning Framework with Values/Guiding Principles

Such a co-developed structured planning framework provides:

- A universal and compelling vision for the future of AI research
- A series of goals that collectively enables the vision to be met
- Subordinate objectives and strategies that are specific and time-bound, which both help to drive activities so that they successfully meet the goals and provide NAIRR and the Executive Office of the President (EOP) the ability to measure progress
- A set of values and principles that guides all subsequent activities

We believe that this approach, as opposed to the original construct found within the draft, will be much more comprehensive and greatly enhance NAIRR's ability to successfully drive intended outcomes.

Specific comments on interim report recommendations:

- [Recommendation 2-2]: Spurring innovation should explicitly name not just "foundational and use-inspired AI research" in general but national objectives-driven AI research, such as U.S. social well-being and equity, health, national security, and the robustness of civic institutions. NAIRR should be strategically filling in the gaps for national objectives that aren't sufficiently driven by market incentives, or that require cooperation.[3]
- [Recommendation 2-2]: MITRE concurs that NAIRR should actively seek to increase the diversity of AI researchers since that could lead to new ways of addressing how to reduce the differential performances exhibited by some AI systems. A NAIRR operator with maturity in its own JEDI (Justice, Equity, Diversity, and Inclusion) efforts will likely have more success in increasing the diversity of AI researchers than one with less mature efforts.

[2] This and subsequent partnership-related recommendations are based on MITRE's experience- and evidence-based practices gleaned from collaboratively designing and operating many forms of partnerships, including PPPs. MITRE recently published a toolkit with these insights, a portion of which is available at: MITRE's Public-Private Partnership Accelerator Toolkit (P3TK). 2022. MITRE, https://ppptoolkit.mitre.org/. Last accessed June 24, 2022.

[3] MITRE Response to OSTP's RFI Supporting the National Artificial Intelligence Research and Development Strategic Plan. 2022. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-01760-16-mitre-response-ostp-rfi-national-artificial-intelligence-research-and-development-strategic-plan.pdf.

- [Recommendation 2-3]: To the extent that NAIRR involves contributions (e.g., expertise, compute, data, funding) from non-government partners, those contributing partners will likely expect to have a role in shaping the nature of the collaboration, including the NAIRR strategy, composition, and value proposition. NAIRR should extend an approach noted in the Interim Report (tying accountability of the management entity to the Board of Governors and external advisory bodies) to drive partner engagement in earlier stage design, prototyping, and operations.[4]

b. Establishment and sustainment of the NAIRR. (Chapter 3 of the report)

MITRE generally concurs with the recommendations of Chapter 3. The envisioned collaborative and cross-sector nature of NAIRR is similar to other PPPs that we have helped establish and maintain over several decades. We have noted that successful PPPs have three primary characteristics:

1. PPPs are working arrangements based on a mutual commitment—over and above that implied in any contract—between one or more public sector organizations and any other organization(s) outside the public sector to achieve some mutually beneficial outcome.
2. PPPs are collaboratives in which the goals, structure, governance, roles, and responsibilities are mutually determined, and decision-making is shared.
3. PPPs are distinct from traditional contractual arrangements and are rooted in co-creation, co-design, and co-resource mobilization.[5,6]

Planning for NAIRR can benefit from the lessons learned and proven practices based on innovation-centric and information-sharing PPPs:[7]

- **Innovation-centric PPPs** focus on applied research and development based on the partners' shared interests in reducing their risk and investment to create new intellectual property (IP) and/or cross the chasm of technology adoption. Examples include tech development consortia, national laboratories, government use of cooperative research & development agreements, and similar approaches to stimulate new solutions or markets.
- **Information-sharing PPPs** focus on collaborative data sharing and integrated analyses to produce insights that are otherwise unavailable elsewhere, so that partners can take action on whole-of-nation challenges (e.g., healthcare delivery, quality, and payment integrity; cybersecurity; transportation safety) and realize benefits to their organization and the public.

MITRE recommends that NAIRR consider the following lessons based on MITRE's Public-Private Partnership Accelerator Toolkit given the importance of cross-sector collaboration in achieving NAIRR outcomes.

[Recommendations 3-8, 3-9]: **Establish and reinforce shared decision-making.** PPPs are fundamentally trust-based journeys. In most PPPs, the public partner(s) (i.e., government agencies) share control of the strategy, operations, and decisions with other members of the partnership. This diffusion of power may sometimes cause tension, but achieving whole-of-nation impact requires trust and some give and take.

[4] Public-Private Partnership Accelerator Toolkit "Value Proposition." 2022. MITRE, https://ppptoolkit.mitre.org/value-proposition/. Last accessed June 24, 2022.

[5] D. Brinkerhoff and J. Brinkerhoff. Public–private partnerships: perspectives on purposes, publicness, and good governance. 2011. Public Administration and Development, https://www.researchgate.net/publication/227724894_Public-private_partnerships_Perspectives_on_purposes_publicness_and_good_governance. Last accessed June 20, 2022.

[6] Reports – Office of Global Partnerships. 2022. U.S. Department of State, https://www.state.gov/reports-office-of-global-partnerships/. Last accessed June 20, 2022.

[7] MITRE adopted this taxonomy of PPPs to differentiate these newer types of PPPs from traditional, infrastructure-centric PPPs. Most PPPs are for developing (and operating) major public infrastructure such as toll roads or water treatment plants—and are accomplished through a long-term, performance-based government contract that places the management and major share of risk on the private entity.

When the public partner is willing to collaborate, be flexible, and share decision-making authority, there can be large-scale impacts. A successful government partner is prepared to execute many important and distinct roles—champion, funder, recruiter, co-chair of governance bodies, and more—and, equally important, is willing to step back and follow industry/academic partners to advance the shared mission and honor the PPP agreements.

[Recommendations 3-6, 3-20]: **Maximize flexibility.** Enable the PPP to evolve organically with operational flexibility. Successful PPPs allow for the adaptation that happens when you allow smart people collaborating under the right partnership model to respond to emergent challenges, innovations, and their own learning. Agreements and governance that explicitly allow for flexibility and responsiveness to partner input and group-based decisions will serve to advance the shared mission and tap into partner strengths as they collaborate, learn, and adapt together.

[Recommendations 3-2, 3-5, 3-13, 3-14, 4-8]: **Explore and define mutual benefit.** Enable PPP partners—entities that represent groups affecting and affected by the PPP's work—to explore through prototypes, proofs of concept, and similar lower-risk trials how the PPP will provide each organization benefits that outweigh the cost and risk of their participation. As part of early shaping of collaboratives, MITRE has found it essential that partners gain (at a high level) a clear understanding of the solution the PPP is intended to deliver and a viable idea for how they collaboratively build that solution. Successful PPPs test the following value propositions early in their collaboration: articulate a common understanding of the group's mission and objectives, aid in recognizing both similar and differentiated benefits of participation, facilitate the buy-in of key partners that will need to help stand up and develop the partnership, and enable the group to share relatable messaging about the PPP's work when ready to recruit new members. Early conversations among partners will include many thoughts about what the group can accomplish together and what those accomplishments mean for them, the entities they represent, and the overall system of which they are a part. These early thoughts will be tested throughout the proof of concept; only some will emerge as the proven value proposition(s) of the PPP. For an example, see the value proposition exploration process for the MDIAS initiative.[8]

[Recommendations 3-7, 3-8, 3-9, 3-12, 3-15, 3-20]: **Manage expectations.** Cross-sector collaboratives succeed when they openly address the unique needs, interests, and concerns of affected groups. Much like partners co-designing the PPP's value proposition, MITRE has found that providing stakeholders a safe space to air and collaboratively address needs, risks, and concerns is a leading indicator of PPP success. PPP experts can facilitate business and legal representatives from partner organizations working together to develop mutually satisfactory agreements (and mitigations to address any concerns) about:

- Purpose, governance, roles and responsibilities, and operations of the PPP
- How information is shared, by whom, and when
- Data privacy, security, and permitted uses
- Invention, ownership, and use of intellectual property
- Responses to legal demands for disclosure, Freedom of Information Act
- Measuring outputs and outcomes, learning, and adaptations
- Conflicts of interest, antitrust, unfair competitive advantage, safe harbor, and any other topics specific to the partnership

[Recommendations 3-8, 3-20]: **Collaboratively define guiding principles.** When partners agree to a set of guiding principles—particularly when they co-define those principles—those norms help the PPP

[8] MDIAS Proof of Concept Overview. 2022. MITRE, https://mdias.org/wp-content/uploads/2022/02/MDIAS-Proof-of-Concept-Fact-Sheet_021122-prs.pdf.

navigate unanticipated issues and gray areas as it operates and adapts to achieve its mission.[9] Example principles include:

- **Strictly for PPP mission** – Partners share funding, expertise, information, and other in-kind contributions solely for the purposes of the stated mission. Partners will not use this information for unfair competitive advantage, punitive reasons, or any other purpose.
- **Collaborative governance** – Partners co-design the partnership concept, operations, and legal agreements for mutual benefit and to protect partners' interests and data. Every partner has an equal voice in the consensus-based decision-making of the partnership. Partners commit to working together in good faith to achieve the goals of the partnership.
- **Protection of partner data** – Partners codify legal, security, privacy, ethical, and other expectations to safeguard their information from inappropriate use or disclosure and obtain commitment that all parties will comply. Partners retain ownership and control of their data; if a partner chooses to end participation, that partner's data is destroyed.
- **Voluntary participation for mutual and public benefit** – Partners voluntarily participate in the partnership predicated on their receiving value from the partnership.
- **Meaningful contributions to transparent operations** – Partners contribute (e.g., time and expertise, information, technology, funding) to the partnership in an equitable and substantive manner, which may vary by task. The PPP operates transparently, with all partners shaping and having access to documented processes, communications, and ways of working together (e.g., collaboration tools and shared AI data/infrastructure).

[Recommendation 3-6, 3-13, 3-14, 4-6]: **Create conditions for trusted collaboration.** If suitably designed, the NAIRR's management entity could effectively serve as a Trusted Third Party (TTP) among government and non-government partners. Regardless, TTPs can convene partners, nurture relationships, guide collaboration, serve as a trustworthy steward and capable analyst of partner data, and as needed mitigate partner concerns about the inappropriate use of their contributions or unintended effects of their participation in the PPP. This is especially true when the TTP is an independent and objective entity that lacks commercial interests or other potential conflicts of interest. Partners are likely to require an independent and experienced TTP when they seek to mitigate concerns such as:

- **Competitive advantage** – If whatever partners share in good faith is used against them by competitors (in or external to the PPP), or PPP participation affects their market position.
- **Adverse action** – If the agency that regulates them is also a PPP partner, industry partners may be concerned that their participation increases their exposure or could be used for punitive purposes.
- **Commercial conflicts of interest** – If partner data were, for example, to be resold or monetized, or the entities who have access to the data also have a financial interest in the same markets.
- **Protecting IP** – If IP owned by partners is misused or if partners contribute to an invention while participating in the PPP.
- **Exposure** – If the sharing and analysis of data or related PPP activities increases perceived or actual privacy, compliance, or legal risk.[10]

[9] For example, the Department of Transportation's Partnership for Analytics Research in Traffic Safety (https://www.nhtsa.gov/parts-partnership-for-analytics-research-in-traffic-safety. Last accessed June 24, 2022).

[10] Note that successful PPPs requiring a TTP also ensure that the TTP follows the safeguards codified in PPP agreements, such as: properly handles partner-provided data; ensures any partner's data is not accessible by any other partner including government partners; uses data only for partner-approved purposes; anonymizes data when needed so that individuals are not identifiable in results and results are not attributable to specific partners; is not subject to Freedom of Information Act; and cooperates with the cognizant partner(s) to resist or limit, to the fullest extent permitted by law, any legal process whatsoever demanding the release of any partner information.

[Recommendation 3-5, 3-6, 3-14]: **Explore co-resource mobilization.** As NAIRR demonstrates value to non-government partners, those partners may choose to (further) invest in NAIRR through in-kind and financial contributions. This model of co-resource mobilization mitigates yearly federal appropriations delays and uncertainties. Moreover, this can create a positive feedback loop where more partners are invested in achieving NAIRR outcomes and driving delivery of results, which fosters continued or additional investment. Recommendation 3-1 addresses funding NAIRR through appropriations to multiple federal agencies, which is critical, but overlooks other approaches to long-term sustainability. Private sector contributions can be substantial and be an organic element of NAIRR resourcing and operation. This funding should be accepted under a framework that enables NAIRR to maintain its independence regardless of the source of its finances. NAIRR should explore with potential partners (e.g., cloud services and technology providers) the conditions favoring a broad range of contributions and the optimal resourcing model given capabilities and constraints.

[Recommendation 3-12, 3-11, 3-13]: **Transparent criteria.** NAIRR should provide guidance on transparent, data-driven approaches and methods for selection of applicants competing for NAIRR resources that will achieve NAIRR's objectives of facilitating research with merit while broadening access and participation to underrepresented and underserved researchers and students. A key objective of NAIRR is to broaden access to the resources necessary to conduct AI research to underrepresented and underserved researchers and students, based on research merit. Yet, a tiered structure for NAIRR access based on the cost of resources requested may not be sufficient to provide some amount of higher-cost resources to underrepresented and underserved researchers and students. MITRE recommends NAIRR provide more detailed guidance on the transparent, data-driven approaches for applying selection criteria to groups and individuals competing for NAIRR resources.

[Recommendation 2-1, 2-4]: **Equitable access.** Achieving equitable access to AI resources requires more than making the resources available to the public via application—NAIRR should include a strategy for outreach to underrepresented researchers and students, as well as a plan to provide application support, since better-resourced groups will have more resources and experience in finding these opportunities and preparing the application.[11] MITRE identified information access and application support as a common theme across federal agencies' Equity Action Plans. When awarding access to limited resources, NAIRR should explicitly include equity considerations in the selection criteria to counter biases in merit assessment; MITRE has internally studied guidance on social equity considerations in benefit-cost analysis for government grant selection. NAIRR could even consider the option of conducting broader competitions to solve challenge problems. These could be conducted with initial seeding of data, capabilities, and resources. The goal would be to help inform the most viable applicants to receive additional funding and resources to take technical topics further for research.

c. NAIRR resource elements and capabilities. (Chapter 4 of the report)

In answering this question, MITRE provides insights from select existing PPPs that can be advantageous to NAIRR planning.

[Recommendation 4-9, 4-10, 4-11]: **Data sharing.** MITRE concurs that negotiating a data use agreement (DUA) involving any sensitive or proprietary data can be complicated and lengthy. Each party has legal obligations and equities that should be respected. However, there are ways to streamline and standardize these types of negotiations in a way that maintains the integrity of the data sets and trust in the parties' relationship. MITRE has been able to accelerate the approval for data sharing when a small subset of representative partners collaborates on framing a common agreement and the partnership adopts it as a

[11] A Framework for Assessing Equity in Federal Programs and Policies. 2021. MITRE, https://www.mitre.org/sites/default/files/publications/pr-21-1292-a-framework-for-assessing-equity-in-federal-programs-and-policy.pdf. Last accessed June 24, 2022.

standard DUA template. Some partnerships use an online portal for DUAs where data requesters and data providers only need to enter information in a few fields. When instances require flexibility, MITRE encourages agility and compromise within the bounds of the partnership agreement and guiding principles.

One example of a MITRE-supported information sharing PPP is the ASIAS program. Launched by MITRE and the Federal Aviation Administration in 2007, ASIAS advances aviation safety by leveraging safety data from across the aviation industry to identify emerging systemic risks and to evaluate the effectiveness of deployed mitigations. ASIAS includes government agencies, aviation stakeholder organizations, aircraft manufacturers, and dozens of airlines and corporate operators. The program obtains and fuses data from these partners and other sources so that safety trends can be identified and addressed before accidents or other serious incidents occur. MITRE safeguards this data, which is de-identified, to foster broad engagement and facilitates the data sharing and analysis aspects of ASIAS.[12]

ASIAS is based on the following guiding principles, which foster trust with participating entities:

- ASIAS information is used solely for the identification, monitoring, and mitigation of systemic safety issues.
- Submitted data is not used punitively.
- ASIAS stakeholders voluntarily submit safety-sensitive data.
- Data are de-identified to preserve anonymity.
- Roles and responsibilities of ASIAS stakeholders are developed collaboratively.
- ASIAS data use is transparent to all stakeholders and supporting organizations.

NAIRR may benefit from developing similar guiding principles for its data repositories in collaboration with the data-providing partners. For example:

- NAIRR data repositories are used solely for the creation, testing, and evaluation of AI-enabled capabilities in a manner agreed to by stakeholders.
- NAIRR stakeholders voluntarily submit AI-related data.
- Data are de-identified to preserve anonymity and protected with appropriate controls for sharing.
- Data are characterized for collection methodology and analyzed for bias and ethics, with this characterization contained in data sheets, model cards, and other governance methods.
- Data use is transparent to all stakeholders and supporting organizations.

NAIRR should additionally incentivize the sharing and collection of public-interest datasets in topics not widely available in the commercial and research AI space, aligned with national objectives such as U.S. social well-being and equity, health, national security, and the robustness of civic institutions.

[Recommendation 4-18, 4-19]: **Purpose-suited testbeds.** MITRE concurs that AI comparison testbeds (real-world test, competition, and living laboratory) that are accessible to partnerships and have a low barrier to entry for smaller research entities are an essential element in advancing AI research. Government-funded AI competitions with shared data sets, evaluation protocols, and use cases have successfully driven research in fields such as Natural Language Processing, Computer Vision, Autonomous Systems, and Decision Support.[13] While these competitions were often focused on a specific domain, they resulted in community data sets and facilitated the sharing of approaches and lessons

[12] Report to Congress: Report on the Status of Aviation Safety Information Analysis and Sharing (ASIAS) Capability Acceleration. 2020. Federal Aviation Administration, https://www.faa.gov/sites/faa.gov/files/2021-11/FAA_Report_on_Aviation_Safety_Information_Analysis_and_Sharing_ASIAS_03312020.pdf.

[13] Examples of organizations hosting organized AI competitions include: NIST Text REtrieval Conference (TREC)—see https://trec.nist.gov/; IEEE International Conference on Acoustics, Speech, & Signal Processing (ICASSP); numerous DARPA programs; and Kaggle competitions—see https://www.kaggle.com/competitions. Last accessed June 24, 2022.

learned. NAIRR has an opportunity to advance a more coherent approach to shared testbeds with more principled test and evaluation, which would enable broader and deeper advances in research.

Testbeds should include documentation covering required/provided data sets and evaluations protocols. Data should be characterized using for example Datasheets for Datasets[14] and be properly curated to guard against perpetuating social biases and inequities, for example, by ignoring considerations of underserved populations and diverse demographics.[15] Each AI technology submitted for testing should include a model card documenting how the technology was trained, on what data, for what purpose, how (with results) the technology has been evaluated to date, etc. In hosting testbeds, NAIRR should promote a principled approach to evaluations that whenever possible maps testing in the lab to real-world requirements. This includes the use of evaluation cards that identify the technology tested and document the protocol(s) and data used along with the results of each test conducted. Testbeds should also chronicle lessons learned over time.

Testbeds should provide a means to protect the AI models through their development and training phases, while safeguarding against data exploitation and poisoning. The testbed should be enabled to safeguard against these and other emerging threats to AI that may corrupt the data and models. The testbed too can provide access to sharable insights on ways to design the data to safeguard against these threats. Threat databases are an active area of work with the MITRE ATT&CK[16] knowledge base, and an area of collaboration specifically for AI-enabled systems within MITRE ATLAS.[17]

[Recommendation 4-24, 4-25, 4-26]: **Educational Tools and Services**. The Generation AI[18] program is a collaborative program (between MITRE, academia, and private industry) to develop students across the United States into thought leaders who can leverage the power of artificial intelligence and accessible data. Students and faculty in the arts, humanities, and social sciences are tackling real-world challenges alongside their peers in data and computer science. In addition to data, partners share computational notebooks, lecture notes, and homework assignments with one another in the Nexus via our lesson exchange. The goal is to broaden the application of AI and deepen the science—creating a continuous feedback loop that drives innovation and economic expansion. Developing and delivering the program provided several key insights that are useful for planning NAIRR's educational services:

- Engaging educators and the future AI workforce requires meeting them "where they are." Rather than focusing on the standard computer science and data science disciplines, the program was able to reach tens of thousands of students across varied disciplines (e.g., fashion design, business) to demonstrate how AI could apply to their differing areas of interest.
- Educators often have limited time and ability to design and implement major changes to their curricula. The greatest opportunities for wider AI education can be delivered by working within existing educational frameworks and integrating smaller, modular lessons that fit to currently defined educational outcomes and lessons.
- As AI educational modules are developed, it is important to have a keen understanding of where educators and students have a level of comfort with coding and other required capabilities. Modules can be designed for educators and students to Use (minimal coding requirements and

[14] T. Gebru, et al. Datasheets for Datasets. 2021. Communications of the ACM, https://cacm.acm.org/magazines/2021/12/256932-datasheets-for-datasets/fulltext. Last accessed June 24, 2022.

[15] MITRE's work on the Maternal Mortality Interactive Dashboard is an example that shows necessity for this consideration. (See https://www.mitre.org/publications/project-stories/can-data-modeling-and-analytics-help-reduce-pregnancy-related-deaths. Last accessed June 24, 2022.)

[16] ATT&CK. 2022. MITRE, https://attack.mitre.org/. Last accessed June 24, 2022.

[17] MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems). 2022. MITRE, https://atlas.mitre.org/. Last accessed June 24, 2022.

[18] Generation AI Nexus. 2022. MITRE, https://ainexus.org/home. Last accessed June 24, 2022.

manipulation), Mod (modifying existing code and text for learning), or Create (developing new code for use in AI development).

d. System security and user access controls. (Chapter 5 of the report)

MITRE generally concurs with the findings and recommendations in Chapter 5. Due to the innovative and likely sensitive nature of the data sets maintained by NAIRR, robust cybersecurity and data protection measures are critical to the success of this effort. The threat landscape is rapidly evolving, and NAIRR's information security team will need to constantly monitor and update security controls to adapt. MITRE concurs with the recommendation that NAIRR adopt a living security plan that evolves with the threat landscape. This security plan should include the adoption of controls from frameworks that partners agree are appropriate for the sensitivity of the data sets; regularly recurring trainings that offer few exemptions from participation and, if so, only based on "testing out;" a clearly defined incident management plan with roles and responsibilities delineated; and an insider threat program that ensures there is no misappropriation or degradation of NAIRR's systems and data sets.

e. Privacy, civil rights, and civil liberties requirements. (Chapter 6 of the report)

MITRE generally supports the findings and recommendations in Chapter 6. In particular, the themes of transparency, fairness, diversity, adequate privacy engineering, and trustworthiness are essential to establishing a research environment that integrates privacy, civil rights, and civil liberties (P/CRCL) into the NAIRR landscape. These themes should be woven together to form the floor, not the ceiling, of any adequate compliance regime.

MITRE has experience in partnerships that require the development and engineering of privacy frameworks to improve performance and efficiencies while maintaining the public trust in the data sets at hand. This has occurred in engagements across a broad spectrum of partnerships—both public and private entities, large and small. As NAIRR determines how it will implement the recommendations for protecting P/CRCL, MITRE strongly advises it to first develop a framework of how it intends to use the AI data in a way that aligns with certain principles—such as ethical boundaries. This framework would provide a guide to those internally benefiting from NAIRR and offer an understanding to the general public tracking the progress from the outside. This concept is not a new approach. In fact, the Office of the Director of National Intelligence produced the "Artificial Intelligence Ethics Framework for the Intelligence Community" in June 2020.[19] The Department of Defense's Defense Innovation Unit released its own "Responsible AI Guidelines" in November 2021.[20] Furthermore, any mature program that is required to calculate privacy considerations closely follows the path of widely accepted frameworks. NAIRR's ability to successfully keep P/CRCL at the forefront will require it to establish an AI P/CRCL framework and weave its principles into all its governance and operational documents.

In addition to the AI P/CRCL Framework, NAIRR must be cautious to balance the need for data privacy and protection with the value of the data sets. Because NAIRR is designed to encourage collaboration among a large pool of data users and an even larger pool of data sets, its success in pushing the innovation envelope requires easy access to data. It is a generally accepted privacy principle that data should be shared only with the lowest number of individuals for the least amount of time using it for the least amount of reasons. However, if NAIRR were to follow that model, then its purpose would not be fulfilled. To mitigate this risk, MITRE strongly encourages NAIRR to:

- Incorporate privacy-by-design principles into the various use cases so that each project can include the necessary P/CRCL protections from the beginning of the AI research life cycle.

[19] Artificial Intelligence Ethics Framework for the Intelligence Community. 2020. Office of the Director of National Intelligence, https://www.dni.gov/files/ODNI/documents/AI_Ethics_Framework_for_the_Intelligence_Community_10.pdf.

[20] Responsible AI Guidelines – Operationalizing DoD's Ethical Principles for AI. 2021. Defense Innovation Unit, https://www.diu.mil/responsible-ai-guidelines. Last accessed June 24, 2022.

- Mandate AI P/CRCL trainings on an annual basis, with limited exemptions for opting out based on the ability to "test out," and where necessary require more specific training for researchers and students handling data with higher sensitivity, such as health data.
- Ensure transparency is prominent with all aspects of NAIRR's responsibilities. This can include hosting public-facing platforms, such as a website and social media accounts, to discuss NAIRR's ongoing efforts, or it can include standing up a Citizen Advisory Committee to receive feedback from those not official NAIRR researchers/students.
- Engage a diverse group of stakeholders—diverse in technical abilities, professional experiences, educational institutions represented, and personal attributes.
- Conduct random audits of access controls to data sets and oversight of research projects to ensure proper adherence to the AI P/CRCL Framework.

f. Ideas for developing a roadmap to establish and build out the NAIRR in a phased approach, and appropriate milestones for implementing the NAIRR. Including data sets, use cases, and capabilities that should be prioritized in the early stages of establishment of the resource.

As we emphasized above in sections a, b, and c, a partner-driven approach to shaping and operating NAIRR is critical to achieving the intended whole-of-nation impact. MITRE strongly recommends that NAIRR engage the right set of partners to co-create (and routinely revisit and revise) a prioritized roadmap based on their collective strengths and insights. Stakeholders' buy-in to any roadmap or plan is largely predicated on their degree of involvement in defining it (i.e., seeing themselves in it as a contributor and beneficiary). MITRE also recommends applying organizational change management practices to ensure that stakeholders are ready and supported in accomplishing this journey together.

g. Other areas relevant to the development of the NAIRR implementation plan.

With diversity and growth as a program goal, MITRE recommends proactive outreach that includes key elements, many of which are captured from the MITRE paper *Designing a New Narrative to Build an AI Ready Workforce.*[21] The government has an opportunity to lead by example in the deployment of responsible AI, and should:

- Define and publicly share its internal governance mechanisms and publicly set expectations with industry partners for deploying AI responsibly.
- Convey legal and ethical accountabilities to the public in a way that describes the responsibility individual decision-makers assume when using any potential system of consequence supporting national security missions.
- Adjust messaging to reflect the values of industry's founders and modern employees, including preservation of civil liberties, the value of civil service, and humanitarianism.
- Develop opportunities proactively through individual engagements with established interest groups and leverage classic communication methods to shape messaging.

[21] R. Hodge, et al. Designing a New Narrative to Build an AI Ready Workforce. 2020. MITRE, https://www.mitre.org/sites/default/files/publications/pr-20-0975-designing-a-new-narrative-to-build-an-AI-ready-workforce.pdf,