Federal Register Notice 86 FR 46278, https://www.federalregister.gov/documents/2021/08/18/2021-17737/request-for-information-rfi-on-an-implementation-plan-for-a-national-artificial-intelligence, October 1, 2021.

Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource: Responses

Response to NSF/OSTP RFI
Submitted by the Atlantic Council GeoTech Center
September 27, 2021

The RFI asks for responses to the following six questions.

1. **What options should the Task Force consider for any of roadmap elements A through I above, and why? [Please take care to annotate your responses to this question by indicating the letter(s) of the item (A through I in the list above) for which you are identifying options.]**

Enhanced trust and confidence in the digital economy is founded upon personal privacy, data security, accountability for performance and adherence to standards, transparency of the internal decision-making algorithms, and regulations and governance for digital products and services. Trust and confidence in the digital economy is diminished by practices that do not protect privacy or secure data, and by a lack of legal and organizational governance to advance and enforce accountability.[1] Data breaches, malware embedded in downloaded apps, unfiltered mis- and disinformation, and the lack of governance models to effectively address these harms all contribute to the degradation of social and civic trust. This degradation undermines economic and civic confidence, is costly,[2] constrains the growth of the digital economy,[3] and has destabilizing effects on society, governments, and markets. Trust and confidence in the digital economy is essential for open societies to function, and for resilience against cascading effects of local, regional, or national economic, security, or health instabilities.

In summary, a key goal of the NAIRR testbed is to ensure, as AI technologies and applications are developed, that he future digital economy—powered increasingly by AI—is trusted, is trustworthy, and that it protects individual privacy and rights. The following table provides specific options for several of the roadmap elements. Each is discussed further in the subsequent sections of this paper.

---

1 Amon, "Toward a New Economy of Trust."

2 World Economic Forum, "Why trust in the digital economy is under threat," accessed March 26, 2021, http://reports.weforum.org/digital-transformation/building-trust-in-the-digital-economy/, citing an estimate by McAfee that the costs associated with cybersecurity incidents approximated $575 billion in 2014; Accenture, *Securing the Digital Economy: Reinventing the Internet for Trust*, 16, accessed March 26, 2021, https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50. Cites five-year loss of foregone revenue from 2019 to 2023 to be $5.2 trillion, calculated using a sample of 4,700 global public companies.

3 Congressional Research Service, *Digital Trade and U.S. Trade Policy*, 11, May 21, 2019, accessed March 26, 2021, https://crsreports.congress.gov/product/pdf/R/R44565; Alan B Davidson, "The Commerce Department's Digital Economy Agenda," Department of Commerce, November 9, 2015, accessed March 26, 2016, https://2014-2017.commerce.gov/news/blog/2015/11/commerce-departments-digital-economy-agenda.html. Davidson identifies four pillars: promoting a free and open Internet worldwide; promoting trust online; ensuring access for workers, families, and companies; and promoting innovation.

Roadmap Element	Options
A. Goals	Emphasize trust and trustworthiness of the digital economy as one develops AI technologies and applications. Make this a central tenet of the testbed.
B. Ownership and administration	Construct a national coordinating office to lead and manage the testbed. This will include public- and private-sector representatives, state and local governments, and international outreach.
C. Governance	Establish an advisory council with representation of all stakeholders. A leadership council would be the primary decision-making group, representing the primary funding sources.
D. Capabilities	Use as a model the secure, distributed, cloud-based information environments developed for the Intelligence Community.
E. Barriers to use of data	Emphasize the need to achieve user-acceptable levels of privacy and trust in how the data are used and how individual rights are preserved as AI-based applications become more widespread.
F. Security requirements	Adhere to federal standards and guidelines for trusted information technology, but with up-to-date implementation practices.
G. Privacy and civil rights	Include privacy-preserving technologies in the priority research goals of the testbed and in demonstrations with real users.
H. Sustainment	Include international partners in the design and evaluation of the testbed and the selection of research agendas. This may include both the private sector and with other nations.
I. Agency roles	This is a national-scale initiative, requiring broad involvement by the federal, state, and local governments. The many stakeholders (owners of data, lead agencies for problem areas, funders of research) all must be involved in the long-term sustainment and management of the testbed.

2. Which capabilities and services (see, for example, item D above) provided through the NAIRR should be prioritized?

The following discussion helps inform the following NAIRR topics:

A. Goals for establishment and sustainment of a National Artificial Intelligence Research Resource and metrics for success.

G. An assessment of privacy and civil rights and civil liberties requirements associated with the National Artificial Intelligence Research Resource and its research.

To enhance trust and confidence in artificial intelligence and other digital capabilities, technologies must objectively meet the public's needs for privacy, security, transparency, and accountability.

The growth of digital economies is changing how trust is valued by institutions, businesses, and the public.[4] The traditional view of trust is expressed in terms of the security of a business transaction. The increase in cyberattacks, identity theft, social media disinformation campaigns, and the use of autonomous decision-making software, introduces new factors that affect trust. Trust in a firm's reputation and ethical practices, privacy protection, and how personal data are used depend on technology, business practices, and the public's perception of how well these components of trust are protected.

Not everyone has the same perception of what is trustworthy. However, reaping the benefits of the digital economy requires a high level of trust among users. Therefore, government and industry should work to enhance the transparency and accountability of digital systems to improve trustworthiness. Challenges include the following: (i) views on personal privacy protection are context-dependent, vary by culture or location, and may be formalized in different terms across nations, regions, and states; and (ii) as automated decision-making algorithms proliferate, new applications reveal trust weaknesses regarding implicit bias, unethical use of personal data, and lack of identity protection.

Trustworthiness needs to be prioritized and empirically demonstrated in the evolving market. Building trust involves educating all participants on the fundamental value of trust in the digital economy and ensuring digital systems reflect individual and societal conceptions of trust. There must be national and international standards for judging how well technologies and systems protect trust. Professional organizations that audit for trust in the digital economy will strengthen accountability.

Finding: The European Union's General Data Protection Regulation uses data protection rules as a trust-enabler.[5]

As European Union (EU) member nations work to conform national rules and laws to the General Data Protection Regulation (GDPR), the European Commission notes that these steps may strengthen trust relationships. Other nations propose that a global framework for cross-border Internet policies may be able to protect data security and privacy while still allowing national laws and regulations as a part of the approach if certain trust relationships are maintained. For both approaches, a set of rules or principles provides the foundation for trust.

---

4 Frank Dickson, "The Five Elements of the Future of Trust," IDC, April 22, 2020, accessed March 26, 2021, https://blogs.idc.com/2020/04/22/the-five-elements-of-the-future-of-trust/.

5 "Communication from the Commission to the European Parliament and the Council. Data protection rules as a trust-enabler in the EU and beyond – taking stock," COM/2019/374 final, European Union, July 24, 2019, accessed March 26, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2019:374:FIN.

The GDPR[6] establishes regulations for data security and privacy that apply to any organization that collects or uses data related to people in the EU. The entire data chain is covered by the GDPR, including data collection, processing, storing, and managing.

The GDPR comprises principles that govern data protection and accountability for those who process data. There are technical measures for data security, and organizational design principles for data protection. Data privacy is expressed in terms of privacy rights, including the right: to be informed, to rectification, to erasure, to restrict processing, to data portability, and to object, and the right of access. There are also rights in relation to automated decision-making and profiling. The governance mechanism centers on Data Protection Authorities that work to align each EU member nation's approach to data security and privacy to conform with the GDPR. These Data Protection Authorities have enforcement powers and the ability to levy fines when a GDPR rule is violated.

Finding: Current approaches to machine learning and big data analytics risk weakening data protection rules.[7]

Data privacy protection is vulnerable to advanced data analytics that can infer personal identifiable information by joining loosely related data sources. As a result, the growing use of current machine learning methods applied to large, multi-source data sets highlights potential limitations in the GDPR where such computational methods can infer data originally made private. The development of new data science capabilities may require research on new privacy-preserving technologies for nations to remain compliant with the GDPR. With increasing amounts of personal medical and genetic information being held in data repositories, this need is urgent.

Finding: Evolving US data privacy approaches consider outcome-based methods, versus prescriptive methods.

The development of data privacy laws in the United States is an evolving patchwork, with more than one hundred and fifty state data privacy laws proposed in 2019.[8] There is no overall federal data privacy law.

---

6 "General Data Protection Regulation," Intersoft Consulting, https://gdpr-info.eu/.

7 T. Timan and Z.Á. Mann, eds., *Data protection in the era of artificial intelligence. Trends, existing solutions and recommendations for privacy-preserving technologies*, Big Data Value Association, October 2019, accessed March 26, 2021, https://www.bdva.eu/sites/default/files/Data%20protection%20in%20the%20era%20of%20big%20data%20for%20artificial%20intelligence_BDVA_FINAL.pdf.

8 "2019 Consumer Data Privacy Legislation," National Conference of State Legislatures, January 3, 2020, accessed March 26, 2021, https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

One instance of federal legislation for data privacy proposed in the 117th Congress[9] includes the following key privacy features, which are viewed as outcome-based.[10]

- Transparent communication of the privacy and data use policy
- Affirmative opt-in and opt-out consent
- Preemption, in which the proposed statute would preempt most state laws with limited exceptions for data breaches, and other limited situations
- A right to action, enforced at the federal or state level, to address alleged violations
- Independent audit of the effectiveness and appropriateness of the privacy policy for each entity providing data services

The National Institute of Standards and Technology (NIST) Privacy Framework describes a risk- and outcomes-based approach to establishing privacy protection practices in an organization. Organizations can vary the technologies and design of the privacy protection aimed at satisfying performance outcomes. This may be advantageous when the technologies and applications are changing at a fast pace, e.g., artificial intelligence (AI) and the Internet of Things (IoT).[11]

Finding: New information technologies compel automated compliance testing.

New information technologies and advanced data capabilities challenge current methods of compliance and enforcement. The variety of new ways to collect, process, and analyze data is increasing at a fast rate, while compliance often is determined on a case-by-case basis by regulatory and legal experts. To keep pace, automated testing for compliance with data privacy regulations is necessary.

Table 1 portrays some of the challenges and solutions for achieving automated compliance testing. This research agenda identifies the following key developments: standards, new privacy-preserving technologies, and automated methods to establish compliance. Privacy-preserving technologies are an active research area, and include the following: secure multiparty computation,

---

9 "Information Transparency and Personal Data Control Act," fact sheet, accessed March 26, 2021, https://delbene.house.gov/uploadedfiles/delbene_consumer_data_privacy_bill_fact_sheet.pdf; Information Transparency & Personal Data Control Act, H.R. 2013 — 116th Congress (2019-2020), accessed April 2, 2021, https://delbene.house.gov/uploadedfiles/delbene_privacy_bill_final.pdf.

10 "Developing the Administration's Approach to Consumer Privacy," *Federal Register*, September 26, 2018, accessed March 26, 2021, https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy; Alan Charles Raul and Christopher Fonzone, "The Trump Administration's Approach to Data Privacy, and Next Steps," Sidley Austin LLP, October 2, 2018, accessed March 26, 2021, https://datamatters.sidley.com/the-trump-administrations-approach-to-data-privacy-and-next-steps.

11 National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0," January 16 2020, accessed March 26, 2021, https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf.

(fully) homomorphic encryption, trusted execution environments, differential privacy, and zero-knowledge proofs.

Table 1. Big Data Value Association Strategic Research and Innovation Agenda

Challenges	Solutions
A general, easy-to-use, and enforceable data protection approach	Guidelines, standards, law, and codes of conduct
Maintaining robust data privacy with utility guarantees	Multiparty computation, federated learning approaches, and distributed ledger technologies
Risk-based approaches calibrating data controllers' obligations	Automated compliance, risk assessment tools
Combining different techniques for end-to-end data protection	Integration of approaches, toolboxes, overviews, and repositories of privacy-preserving technologies

Source: Timan and Mann 2019[12]

The value of privacy-preserving technologies involves trade-offs between privacy and utility—how useful is the resulting data—both of which are context dependent.[13] Affecting these trade-offs are the technical methods, the technical definitions of privacy, and the specifications of the privacy laws. The technical methods (e.g., anonymization, sanitization, and encryption) operate on data in different ways. The technical definition of privacy varies by application and the user's perceptions of risk versus the benefit of making personal data available. Privacy laws vary across nations, challenging the uniform application of technical methods. For both professionals and members of the public, making trade-offs between privacy and utility remains challenging. This is partially due to the absence of definitions of and standards for measuring privacy and the social benefits obtained from making data available for use by others.

Priority: Trust and confidence in digital capabilities requires businesses and governments to focus on the responsible use of technology.

Increasing trust and confidence in emerging technologies, such as AI, requires a recognition by both businesses and governments that they have an obligation to use technology responsibly, ensuring that technology has a positive impact on society, especially with regards to equality and

12 Timan and Mann, *Data protection*.

13 Daniel Bachlechner, Karolina La Fors, and Alan M. Sears, "The Role of Privacy-Preserving Technologies in the Age of Big Data," proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, San Francisco, December 13, 2018, accessed March 26, 2021, https://www.albany.edu/wisp/papers/WISP2018_paper_11.pdf; Felix T. Wu, "Defining Privacy and Utility in Data Sets," *University of Colorado Law Review* 84 (2013), accessed March 26, 2021, http://lawreview.colorado.edu/wp-content/uploads/2013/11/13.-Wu_710_s.pdf.

inclusion.[14] Developing and innovating responsibly means ensuring that (i) ethical frameworks and policies exist to guide organizations during all aspects of a product's development and deployment, (ii) fairness in design is emphasized from the outset, and that (iii) questions around the manner in which technologies will be used are given the same rigorous examination as technical issues. As technological capabilities evolve and become more deeply intertwined in all aspects of society, businesses and governments must put ethics at the center of everything they do.

Priority: Build in trust-enabling technologies, measure performance against standards, conduct independent compliance audits.

The digital economy relies on achieving a high level of trust and confidence on a continuing basis as technologies evolve. Trust and confidence-enabling technologies must be developed and built into the components of the digital economy infrastructure; a detailed understanding of the trade-offs between privacy versus utility is an essential foundation. Such technologies must be paired with similar civic norms, practices, and rules designed to enhance confidence in the digital economy. To assure businesses that they remain compliant with data protection regulations as they modernize their practices, automated compliance testing, accompanied by standards of performance, is needed. To establish transparency for automated decision-making algorithms, standards for the measurable performance, i.e., the output results, are necessary. Independent assessments of the compliance testing and algorithmic transparency by professional auditing organizations could enhance trust among all participants in the digital economy and aid accountability and governance; such methods should be explored. However, mechanisms for compliance testing and auditing by regulators are also necessary.[15]

3. How can the NAIRR and its components reinforce principles of ethical and responsible research and development of AI, such as those concerning issues of racial and gender equity, fairness, bias, civil rights, transparency, and accountability?

Recommendation: Assess standards relating to the trustworthiness of digital infrastructure.

Congress should direct an assessment by the National Academies of Sciences, Engineering, and Medicine of the current national and international standards relating to the trustworthiness of digital infrastructure to support the digital economy. "Trustworthiness of an information system is defined as the degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality,

---

14 Kirsten Martin, Katie Shilton, and Jeffrey Smith, "Business and the Ethical Implications of Technology: Introduction to the Symposium," *Journal of Business Ethics* 160, 307–317 (2019), accessed April 16, 2021, https://doi.org/10.1007/s10551-019-04213-9

15 Nicholas Confessore, "Audit Approved of Facebook Policies, Even After Cambridge Analytica Leak," *New York Times*, April 19, 2018, accessed March 26, 2021, https://www.nytimes.com/2018/04/19/technology/facebook-audit-cambridge-analytica.html.

integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats."[16]

Due to the increasing complexity of the digital infrastructure, the assessment should also review design standards for complex systems-of-systems from the perspective of trustworthiness. The overall assessment focuses on systems that support the digital economy. The study should assess the sufficiency of existing standards to guide improvements in trustworthiness, identify where new standards are needed, and recommend the data collection and testing methods that would enable ongoing assessments.

Recommendation: Produce a framework for assessing ethical, social, trust, and governance considerations associated with specific current and future use cases for AI.

The administration should request the National Academy of Sciences to produce a framework for assessing ethical, social, trust, and governance considerations associated with specific current and future use cases for AI solutions. The framework should identify where new federal standards and rules are needed. This guidance should be developed with the participation of relevant executive branch departments and agencies, and in consultation with private industry, academia, members of the public, and government and industry representatives from foreign partners.

Recommendation: Educate the public on trustworthy digital information.

Congress should establish a grant program led by NSF for the purpose of developing a curriculum on trustworthiness of information—distinct from the trustworthiness of information systems—in the digital age. This curriculum should be created by a consortium headed by a university or coalition of universities. The program should be administered by select universities, with the participation of US information providers. The goal should be to educate the public on how to assess the trustworthiness of information—its credibility, truthfulness, and authenticity, and to develop tools that students and members of the public can use and benefit from on a regular basis.

4. What building blocks already exist for the NAIRR, in terms of government, academic, or private-sector activities, resources, and services?

Recommendation: Create measurement methods and standards for evaluating trust in the digital economy.

The administration should direct the National Institute of Standards and Technology (NIST) to establish methods for evaluating users' trust in the digital economy given the increasing use of AI, big data analytics, and automated decision-making algorithms. This work builds on the Commission on Enhancing National Cybersecurity's *Report on Securing and Growing the Digital*

[16] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5, September 2020, accessed April 16, 2021, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Economy[17] and the *National Strategy for Trusted Identities in Cyberspace*.[18] One assessment framework example[19] describes measures of: "(i) user trust in the digital environment, e.g., data privacy, security, private sector efforts to control the spread of misinformation, and private sector adherence to cybersecurity best practices; (ii) the user experience, i.e., the effort needed to interact with the digital environment; (iii) user attitudes, e.g., how trusted are government and business leaders; and (iv) user behavior, i.e., how much do users interact with the digital environment."

The administration should create a coalition to develop international standards for achieving trust in the digital economy. The coalition should include representatives from NIST, the Federal Trade Commission (FTC), private industry, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), and international standards organizations. The United States and like-minded nations and partners should develop national assessments of trust in the digital economy using these standards.

Recommendation: Empower an organization to audit trust in the digital economy.

Congress should establish or empower an organization to audit the efficacy of measures designed to ensure trust in the digital economy and assess conformance to current and future standards designed to enhance and maintain such trust. Independent third parties or the Government Accountability Office (GAO) are examples of where such auditing organizations could be housed.

As part of this process, the auditing organization could provide recommendations to Congress on legislation that would enhance existing trust measures, develop new trust measures, and create trust performance standards. The auditing organization should also provide a mechanism through which the public and industry can raise topics and concerns for attention and, for cases where assessments or audits were done, include an ombudsman function for assessment appeals, identification of new information, or adjudication of concerns in a manner distinct from political influence.

The administration should work to establish a similar auditing program with EU members of the International Organization of Supreme Audit Institutions.

---

17 Commission on Enhancing National Cybersecurity, *Report on Securing and Growing the Digital Economy*, December 1, 2016, accessed March 26, 2021, https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.

18 White House, "National Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy," April 2011, accessed March 26, 2021, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

19 Bhaskar Chakravorti, Ajay Bhalla, and Ravi Shankar Chaturvedi, "How Digital Trust Varies Around the World," *Harvard Business Review*, February 25, 2021, accessed April 16, 2016, https://hbr.org/2021/02/how-digital-trust-varies-around-the-world#:~:text=To%20that%20end%2C%20in%20partnership,user%20experience%3B%20the%20extent%20to.

5. What role should public-private partnerships play in the NAIRR? What exemplars could be used as a model?

Recommendation: Conduct demonstration projects involving artificial intelligence to improve delivery of public- and private-sector services at local, state, and federal levels.

Congress should authorize and appropriate funds for AI demonstration projects that improve the delivery of public services.[20] The overall program would be managed by one of the National Laboratories or by a newly created FFRDC with the mission to leverage technology to improve the delivery of public services. These testbed projects would be supported by local and state grants, cross-cutting federal government efforts, and public-private partnerships (PPPs) to employ AI to improve healthcare, workforce training, food production and distribution, and other areas. The overarching goals are to increase public trust in, understanding of, and confidence in AI; to learn how to use AI in ways that reduce inequality and enhance, rather than replace, human work; and to improve access, affordability, and availability of such services. At local, state, and federal levels, individual government agencies will gain long-term benefits by acquiring the necessary data infrastructure to employ AI to improve the delivery of public services.

6. Where do you see limitations in the ability of the NAIRR to democratize access to AI R&D? And how could these limitations be overcome?

Recommendation: Develop privacy-preserving technologies for the digital economy and demonstrate in a full-scale test their conformance with the General Data Protection Regulation.

The administration should direct NIST to establish and test privacy-preserving technologies that enable a risk- and outcomes-based approach to trust in the digital economy. The test should evaluate, at scale, conformance with relevant GDPR rules, conformance with existing US laws governing data privacy, and robustness with respect to innovations and advances in information technologies and data capabilities, especially those based on AI, machine learning, and the IoT. This work should include the development of technical definitions of privacy and application-specific measures of the utility of analyses that are based on privacy-protected data. The tests should include end user evaluations.

The administration should establish a near-term program that demonstrates privacy-preserving technologies to aid the trusted collection and sharing of data for the purpose of improving individuals' access to healthcare during large-scale biological events. This program should be jointly managed by NIST, the Department of Health and Human Services (HHS), the National Institutes of Health (NIH), and the National Science Foundation (NSF). This program will monitor system performance to inform the development of standards for the ethical use of the shared data and how data governance will be formulated.

---

[20] A potential source for the types of initiatives of interest is the OECD Network of Experts on AI (ONE AI). This group provides policy, technical and business expert input to inform OECD analysis and recommendations. "OECD Network of Experts on AI (ONE AI)," OECD.AI, accessed March 26, 2021, https://www.oecd.ai/network-of-experts.