National Artificial Intelligence Association

NAIA Comments to OSTP re AI Action Plan

This document is approved for public dissemination. The document contains no business-proprietary or confidential information. Document contents may be reused by the government in developing the AI Action Plan and associated documents without attribution.

About NAIA

The National Artificial Intelligence Association (NAIA) is a 503(c)(6) nonprofit organization that focuses on ensuring opportunities and global competitiveness for American businesses developing or using artificial intelligence ("***AI***"). Our membership is comprised of 400 public & private businesses, legislators, financial institutions, educational organizations, nonprofit organizations, healthcare providers, community organizations, small businesses and other stakeholders.

Our Comments

Our comments were developed with our leadership and members by our General Counsel, Steve Britt, Managing Partner of Britt Law LLC (steve@thenaia.org) (www.brittlawllc.com), who holds the AIGP, CIPP/Europe and CIPM certifications for artificial intelligence & data privacy.

A. Our Key Priorities

We applaud the Trump Administration for conducting an analysis of the complex regulation of cyber, data privacy & AI (collectively, "***data management***") with the REQUEST FOR INFORMATION ON THE DEVELOPMENT OF AN ARTIFICIAL INTELLIGENCE ACTION PLAN (the "***RFI***").

The RFI represents a unique opportunity to reset the laws & regulations applicable to every organization's use of data, whether in the government or the private sector. Our comments are based on the following priorities:

1. Support the Trump Administration's goal of ensuring US global dominance of all forms of technology development, including AI,

2. Enhance the security of all US assets and operations,

3. Stimulate innovation & investment in technology development by eliminating conflicting laws that burden companies with unnecessary compliance costs,
4. Simplify data privacy rules through adoption of a CLEAR (CERTIFIED LABEL FOR ELECTRONIC AGREEMENT RIGHTS) Label that implements *privacy by design* principles,
5. Make AI development transparent through principles that empower consumers to manage their own risks,
6. Codify Federal law that preempts all state laws & regulations relating to data management,
7. Stimulate "all the above" energy production, including development of modular nuclear energy & advancement of lower energy consuming quantum computing,
8. Protect our youth from the adverse mental health effects of social media platforms and addictive designs of phones, apps, software, tools & games,
9. Make the US Government the most efficient on earth, powered by AI and
10. Ensure Open-Source Intelligence remains open for all companies large & small.

B. <u>Outline of our Comments</u>

A. Our Key Priorities

B. Outline of Comments

C. Current Legal Landscape

   a. GDPR

   b. EU AI Act

   c. State AI Acts

   d. State Data Privacy Laws (including TRAIGA)

   e. American Privacy Rights Act of 2024

D. [*Proposed*] American Data Management & AI Act ("***ADMAIA***")

E. NAIA's Recommendations

F. Appendix: Form CLEAR Label

C. Current Legal Landscape

We begin with a review of the data management laws that have passed since 2022. We believe this landscape explains the need for action and why the RFI is so timely.

a. **GDPR.** All data protection roads begin here. Effective in 2018, GDPR automatically applies to all 27 EU member states and the collection of data by both profit & nonprofit organizations, both online and offline. It applies to the collection of EU data by any organization located anywhere in the world, including online.

   GDPR taught us about data subject rights (right to know, correct, limit, opt-out, access & delete) that are now included in every US data privacy law.

   Article 25 of the GDPR ("***privacy by design***") required the implementation, by default, of designs that are the most protective of data privacy. This requirement was not included in the California Consumer Privacy Act ("***CCPA***") nor any state data privacy law since. If ***privacy by design*** had been included in US data privacy laws, it would have simplified and clarified the data regulation path we have been traveling. We believe it should be part of a new regime going forward.

b. **EU AI Act.** The EU AI Act applies to general purpose AI ("***GPAI***") models and to "high risk" AI models that are introduced into the EU or used by Europeans. It governs the following levels of risk to users' fundamental rights: (i) "***prohibited***" *uses*" (*e.g.,* deceptive techniques, social scoring, predictive policing, real time biometric I.D. by law enforcement and scraping images for facial recognition databases), (ii) "***high risk***" uses involving critical infrastructure, access to education, employment, public-private benefits and democratic processes, and (iii) "***low or minimal risks***," which are systems that generate images, audio-video or text.

   Providers of high-risk and GPAI systems with systemic risk must (i) implement *and document* a responsible AI risk management system, (ii) train and continuously test the system with valid high-quality data, (iii) validate the system before release and throughout its lifecycle as being "***accurate***," "***robust***," "***transparent***," "***secure***," "***unbiased***" and "***accountable***," (iv) document how the algorithms work, (v) perform an EU AI Act compliance assessment before release, and (vi) register the system in an EU-wide database. Fines for violations of the Act can reach €15,000,000 or 3% of worldwide revenue, whichever is higher.

c. **State Artificial Intelligence Laws.** In the absence of a Federal AI law, states are enacting their own AI laws. The first movers are Colorado, Utah, Texas & California:

   Colorado Artificial Intelligence Act

   Colorado's AI Act takes effect on February 1, 2026 and mirrors the EU AI Act. It requires developers of high-risk AI systems to prevent algorithmic discrimination

based on a person's age, color, disability, gender, race, religion or veteran status.

High-risk AI systems are those that make or substantially contribute to the making of a "***consequential decision***," which is any decision that affects access to or the price of education, employment, financial services, government services, healthcare, housing or insurance.

Colorado AI Developers must document the proper and foreseeable harmful uses of the AI system, explain the type and lineage of system training data, report on the logic of the algorithms, explain risk mitigation measures, publish a statement that details how the system was developed and how it manages known or foreseeable risks, and promptly report instances of algorithmic discrimination to the A.G.

Utah Artificial Intelligence Act

Utah 's artificial intelligence law took effect on May 1, 2024 and primarily covers generative AI, which it subjects to Utah's consumer protection laws. A person using generative AI in a business regulated by the Utah Division of Consumer Protection must disclose, ***if asked***, that the user is interfacing with a machine. A person providing the services of a licensed occupation must ***affirmatively inform*** consumers they are interacting with AI.

<u>California AI Acts and Cyber, Risk & ADMT Regulations</u>

In 2024, California passed several AI laws, including the following:

(i) **AI Training Data Transparency Act:** Effective January 1, 2026, developers of generative AI models must publicly post on their web site information about the training data used in their systems, including the sources of the data, the types of data points, any applicable IP rights to the data, whether the datasets contain personal information and any modifications to the model.

(ii) **(SB 942) California AI Transparency Act:** Also on January 1, 2026, generative AI systems that produce audio-video content with 1,000,000 or more monthly users must make an AI detection tool publicly and freely available to users that reveals the system's creation or alteration of content.

(iii) **(AB 1008) Amendments to CCPA:** CCPA was amended to cover personal information in AI models, giving data rights to AI data, tokens and weights.

In addition, the California Privacy Protection Agency ("***CPPA***") is proposing the following regulations for activities posing a significant risk to consumer privacy:

- **Cybersecurity Audits**

Every business processing data that poses a significant risk to consumers must

complete an annual cybersecurity audit of key security controls performed by a qualified independent professional that is reported to the BOD or CEO.

- **Risk Assessments**

Every business whose processing of data poses a significant risk to privacy must also conduct a risk assessment. "***Significant risk to privacy***" means (i) selling or sharing personal information, (ii) processing sensitive information, (iii) using automated decision-making technology ("***ADMT***") for significant decisions or for extensive profiling, or (iv) using personal information to train ADMT or an AI system. The assessment must weigh the risks of data processing activities against their benefits with risk mitigation actions. It must explain the quality of the data, the logic of the algorithms and the use of system outputs. An abridged version of the assessment must be submitted to the CPPA.

- **ADMT Regulations**

A business that uses ADMT for "***significant decisions***" about a consumer regarding financial services, housing, insurance, education, employment, compensation, healthcare or for extensive profiling must comply with new ADMT regulations. Consumers must be provided a "***Pre-Use Notice***" of the purpose of the ADMT, the consumer's right to opt out of such use, how the ADMT works, its logic, its intended outputs and how the business will use those outputs. Consumers have a right to appeal an automated decision to a qualified human reviewer with the power to overturn the decision.

d. **State Data Privacy Laws.**

In the 7 years since GDPR, we have no Federal data privacy law but 23 state data privacy and "***consumer health data***" laws. While independent and complex, these laws actually share many similar terms.

For example, with rare exception, they all require covered businesses to (i) fully disclose all categories of personal information collected, (ii) provide broad data subject rights, (iii) restrict the collection and use of sensitive data, (iv) control the transfer of data for targeted advertising and profiling, (v) require reasonable data security, and (vi) require broad data protection assessments that must be available to regulators on request.

Nevertheless, these similarities are overtaken by a wide range of conflicting or inconsistent terms.

For example, (i) some state laws apply to non-profit organizations while most do not, (ii) some require prior opt-in to the collection and use of sensitive information while others require a right of opt-out to such activities, (iii) some regulate online activities

impacting the mental health of minors and others do not, (iv) the age of minority varies by state, (v) the response deadlines for data access requests vary, (vi) some states mandate automatic notice to regulators for denials of a deletion request while others do not, (vii) the CCPA applies to employees and B2B contacts whereas all other states exclude those categories of users, (viii) some states require prior notice and a right to cure for violations of the act while others have no right to cure, (ix) all states require disclosure of the "categories" of personal information collected while only California provides a list of categories, and (x) Washington State requires a separate consumer health data privacy notice under the Washington My Health My Data Act ("***WMHMDA***").

Perhaps the starkest difference in state data privacy laws are the jurisdictional triggers for applicability based on the number of records of the state's residents collected each year, as summarized below:

States	**Annual # of residents from whom personal data is collected**
California, Colorado, Connecticut, Virginia, Utah, Minnesota, New Jersey, Iowa, Oregon, Indiana, Kentucky	100,000
Rhode Island, Maryland, New Hampshire, Delaware	35,000
Tennessee	175,000
Montana	50,000
Texas, Nebraska	One (1) resident
Florida	$1B in revenue

Texas is the next data privacy law expected to pass in the form of the **Texas Responsible AI Governance Act (HB 1709) (TRAIGA).** Introduced in December 2024, TRAIGA would regulate the use of "***high-risk***" AI systems that make or substantially contribute to "***consequential decisions***" (same as the Colorado AI Act). Developers must use reasonable care to avoid algorithmic discrimination and conduct annual risk reviews. They must disclose the (i) purpose of the system, (ii) the nature of consequential decisions made by the system, (iii) the factors used in consequential decisions, and (iv) the identity of the deployer.

Almost all state data privacy laws preclude a private cause of action for violations of the laws. The notable exception is Washington's My Heath My Data Act. With no direct path to sue, the plaintiff's bar has sought out alternatives, resulting in a series of class actions filed under state consumer protection, wiretapping, the Video Privacy Protection Act, common law privacy and California Invasion of Privacy Act.

Turning to AI, no AI Act changes traditional product liability, strict liability and negligence (tort) laws for damages resulting from the use of AI. Given the complexity of AI compliance, AI development is definitely facing substantial litigation risks.

e. **American Privacy Rights Act of 2024 ("APRA").** The APRA (HR 8818) was introduced on June 25, 2024. After two full committee markups failed, the bill died upon expiration of the 118th Congress. Many elements of ARPA were quite reasonable. For example, it applied to:

(i) Businesses governed by the FTC, including certain nonprofits, and exempted small businesses with <$40,000,000 in annual revenue,

(ii) Large data holders with over $250,000,000 in annual revenue or which collected data on more than 5,000,000 individuals,

(iii) It included broad definitions of personal information and sensitive data and granted broad data subject rights,

(iv) Targeted advertising was limited to (i) the specific purpose of the data collection or (ii) express user consent,

(v) On the 2 key issues, APRA preempted state data privacy laws but the exceptions to preemption were many, including consumer protection, employee & student privacy, civil rights, data breach, banking & wiretapping laws, and

(vi) ARPA did authorize a private cause of action for actual damages, attorneys' fees and injunctive relief effective 6 months after passage.

D. [NAIA's Proposed] American Data Management & AI Act ("*ADMAIA*")

The RFI offers a unique opportunity to reduce the barriers to innovation and sound regulation resulting from the random roll out of data privacy and AI laws. All businesses run on data and the current landscape creates a "***Catch 22***" for businesses trying to comply with these laws. Advertising and marketing technologies are ground zero for these issues and, while those are key industries, a new law could unlock the conflict in these regimes from user data rights.

With these goals in mind, NAIA recommends that the Trump Administration propose to Congress and support enactment of a comprehensive data management & AI bill named the "***American Data Management & Artificial Intelligence Act***," or "***ADMAIA***"). Key elements of ADMAIA are set forth below:

a. <u>One Comprehensive Bill</u>. We need a comprehensive solution so ADMAIA would (i) memorialize the data rights of consumers that have reached consensus among EU and state laws, (ii) standardize the consent rules for sensitive data, targeted advertising & profiling, (iii) incorporate privacy by design that enables adoption of a data privacy nutrition label, (iv) preempt all state laws in all related data management and AI areas, including consumer protection, wiretapping and state privacy laws, (v) incorporate responsible AI development principles in a rational manner with self-certification for standards that are not yet established, (vi) standardize all data protection and AI risk assessments, (vii) shield US technology firms from regulatory overreach, and (viii) provide a sound liability regime that protects victims of AI discrimination while protecting innovation with appropriate enforcement mechanisms but with no private cause of action.

b. <u>Data Privacy Regulation</u>.

(i) Incorporate *privacy by design* into all commercial technology development,

(ii) Implement a ***CLEAR Privacy Label*** (Certified Label for Electronic Agreement Rights) for a standardized disclosure of data privacy & AI practices with exceptions based solely on consent & the original collection purpose,

(iii) Establish by default that individuals own and control their personal data unless they voluntarily share, grant or consent to alternative uses,

(iv) Require a uniform set of data rights (right to know, correct, limit, opt-out, access & delete) and eliminate anomalies,

(v) Eliminate record collection tests for applicability of the law and limit a gross revenue test to a small business exemption,

(vi) Ban online use of dark patterns (i.e., the use of an interface that subverts or impairs user autonomy or choice),

(vii) Preempt all state data privacy laws & regulations as applied to data use, including consumer protection, invasion of privacy, employee privacy, consumer health data, wiretapping, video protection and similar laws,

(viii) Preserve exemptions at the entity level for businesses regulated by HIPAA, GLBA, FERPA, FCRA, FCC & FTC but eliminate overlaps where data is regulated by both Federal law and state data privacy laws,

(ix) Apply to nonprofit organizations subject to defined safe harbors,

(x) Provide small business exemptions from burdensome requirements,

(xi) Merge requirements for data protection and AI risk assessments under regulator-approved forms, and

(xii) Adopt a common data security audit framework.

c. Artificial Intelligence Regulation.

(i) Prioritize transparency in AI development over assessments performed before product completion,

(ii) Establish responsible AI development principles for Federal government acquisition and use of AI technologies,

(iii) Promote the development of AL/ML by (A) forming a national computation reserve/resource for small business & research institutions, (B) incentivize the sale of data to the Federal government for open-source AI/ML training, and (C) establish favorable data rights clauses for AI/ML developed with government-provided compute or data resources,

(iv) Ensure secure export controls on international distribution of AI technologies and remote access to AI technologies,

(v) Expand access to Free and Open-Source Software (FOSS) under *permissive* licenses and Responsible AI Licenses (RAIL), limiting application of *copyleft* licenses to AI models,

(vi) Promote use of synthetic training data and informed human-in-the-loop for overly burdensome safety, transparency and nondiscrimination standards,

(vii) Require use of valid training and test data and require ongoing monitoring and validation of AI models throughout their life cycle,

(viii) Codify that data minimization does not prevent the use of LLMs, that training data may be retained for extended periods and that databases may be reused if data was collected lawfully and reuse is compatible with the original collection purpose,

(ix) Merge AI risk & compliance assessments with data protection assessments,

(x) Require disclosure of all generative AI uses with appropriate content alteration and watermarking requirements,

(xi) Impose trustworthy AI standards of security, resilience, transparency, explainability, lack of bias and human centricity, and

(xii) Require validation of IP rights, developer's right to model inputs & outputs and any use of public AI development platforms.

d. Enforcement.

(i) Permit audits & investigations by state attorneys general and regulators enforcing Federal (*i.e.,* ADMAIA) standards, fines & penalties,

(ii) No private cause of action for violations of ADMAIA but any claims authorized should be limited to (i) recovery of actual damages, with (ii) no right to special or punitive damages, and (iii) subject to a 60-day right to cure before an action can be filed, and

(iii) Protect EU-US Data Privacy Framework ("***DPF***") for transfers of EU personal data to the US by filling vacancies on the Privacy & Civil Liberties Oversight Board ("***PCLOB***"), (2) protecting CJEU adequacy decision for the DPF, and (3) supporting FTC and DOJ enforcement of FISA Section 702, and

(iv) Pursue a joint US-EU regulatory regime similar to DPF to harmonize data management enforcement by US & EU regulators for ADMAIA, GDPR, Data Act, Data Services Act & Data Markets Act.

e. Children's Privacy Rights.

(i) Require informed parental consent for online services that collect, use or disclose the personal information of children under age 18 with detailed disclosure obligations to parents as a condition to their consent,

(ii) Expand definition of children's personal information to include biometric identifiers (fingerprints, retina, voiceprints, etc.) and GPS location data,

(iii) Impose strict limits on sharing of children's data for targeted advertising,

(iv) Require social media companies to employ design features that prevent addictive behavior like time limits and restrictions on addictive features, and

(v) Increase fines and penalties for noncompliance.

f. Energy.

AI requires stable, consistent, non-breaking power. Nuclear is the only reliable source and NAIA encourages the Administration to fund pilots of nuclear-

powered data centers and streamline licensing to deliver safe nuclear energy to meet AI's rapidly rising electricity demands.

E. NAIA's Recommendations

The National Artificial Intelligence Association strongly supports the Trump Administration's vision of American global leadership in AI technology development. We advocate for policies that maintain competitive advantages, strengthen R&D ecosystems, foster talent development, and secure critical technologies. Strategic investments in emerging AI capabilities must be coupled with removing innovation barriers to ensure that the US remains the unrivaled world leader in artificial intelligence development and deployment.

NAIA's proposed legislation, ADMAIA, seeks to level the regulatory playing field for US businesses in order to enable efficient and effective compliance. We believe that passage of a broad new Federal data privacy & AI law will restore the US as a global leader of sound and innovative technology development.

In addition, enhanced security of US assets and operations requires a comprehensive approach integrating AI-driven threat detection and response capabilities across critical infrastructure. We recommend robust cybersecurity frameworks embracing zero-trust architecture, increased public-private intelligence sharing, and protection of intellectual property. Advanced AI systems can proactively identify vulnerabilities, detect anomalies in real-time, and automate incident response, creating a security posture that safeguards America's technological and economic interests.

Innovation requires freedom from excessive regulation. We advocate eliminating conflicting laws that create compliance burdens, particularly those imposing duplicative requirements across agencies and jurisdictions. A streamlined regulatory approach will reduce compliance costs, allowing companies to redirect resources toward groundbreaking research and development. This regulatory rationalization will accelerate AI advancement while maintaining appropriate guardrails through performance-based standards rather than prescriptive requirements.

The CLEAR Label framework outlined in ADMAIA and shown in the attached Appendix would transform data privacy by implementing "*privacy by design*" principles through a standardized, consumer-friendly labeling system. This approach would communicate data practices transparently while simplifying compliance across jurisdictions. CLEAR Labels would indicate precisely what information is collected, how it's used, and consumer control options—similar to nutrition labels—enabling informed consent without burdensome paperwork. This balanced approach protects consumers while enabling innovation.

Transparency in AI development requires empowering consumers to understand and manage their own risk tolerance. We advocate for clear disclosures about AI capabilities

and limitations, opt-in mechanisms for sensitive applications, and tools that allow individuals to customize AI interactions according to their preferences. **This consumer-centered approach maintains innovation momentum while building public trust through education and meaningful control options.**

Federal preemption of state data management laws is essential to eliminate the current patchwork of conflicting regulations. A unified national framework would provide consistent protection while reducing compliance complexity and costs. This approach would establish clear national standards for data collection, processing, security, and consumer rights, creating certainty for businesses while ensuring that all Americans receive an equal and effective level of data protections regardless of geographic location.

America's AI leadership depends on next-generation computing infrastructure. We advocate accelerating development of an “all-the-above” energy production policy with specific focus on modular nuclear reactors to provide clean, reliable energy for data centers and quantum computing facilities. Strategic investments in energy efficient data centers and quantum technologies will unlock computational capabilities essential for advanced AI applications with less energy consumption. This dual-track development approach ensures America maintains both the energy capacity and processing power necessary for next-generation AI systems.

Protecting youth mental health requires balanced policies addressing harmful design elements in digital platforms. We support research-driven standards that prevent exploitative patterns in apps, games, and social media without stifling innovation. This includes promoting transparency about engagement metrics, limiting certain addictive features for minors, and developing age-appropriate design codes. These protections should be developed in partnership with industry to ensure effectiveness and practicality.

Transforming government efficiency through AI requires strategic implementation of automation, predictive analytics, and intelligent decision-support systems across federal agencies. We advocate a coordinated approach to digitize processes, eliminate redundancies, and enhance service delivery. This would reduce operating costs, improve user experience, and enable data-driven policymaking.

Finally, Open-Source Intelligence must remain accessible to businesses of all sizes. Policies should ensure that foundational AI research, datasets, and basic algorithms remain broadly available while protecting proprietary inventions. This will prevent monopolization of critical AI building blocks, foster competition, and help small businesses participate in AI advancement. Democratized access to core AI strengthens American innovation.

Thank you for the opportunity to submit these Comments. We look forward to discussing these issues further.

Sincerely, NAIA

Appendix: Sample CLEAR Label

Here's a conceptual "Nutrition Label" for data collection permission documents, aiming for clarity and transparency:

Data Collection Permission Facts

Serving Size: One Document (per individual/organization)

Amount Collected Per Serving:

Contact Information: (Check all that apply)**

* [ ] Name
* [ ] Address
* [ ] Email Address
* [ ] Phone Number

Demographic Information: (Check all that apply)**

* [ ] Age
* [ ] Gender
* [ ] Location (e.g., City, State, Country)
* [ ] Occupation
* [ ] Education Level

Device Information: (Check all that apply)**

* [ ] Device ID
* [ ] IP Address
* [ ] Browser Type
* [ ] Operating System

Usage Data: (Check all that apply)**

* [ ] Website Activity (e.g., Pages visited, time spent)
* [ ] App Usage (e.g., Features used, frequency)

* [ ] Search Queries

* [ ] Purchase History

Sensitive Information: (Check all that apply - Requires Explicit Consent)**

* [ ] Health Information

* [ ] Financial Information

* [ ] Biometric Data

* [ ] Religious Beliefs

* [ ] Sexual Orientation

Other Data: (Specify)** _____

% Daily Value*

Purpose of Collection: (Describe in clear, non-technical language)**

* _____

Data Retention Period: (How long will the data be kept?)**

* _____

Data Sharing: (Who will the data be shared with?)**

* [ ] Third-Party Partners (List categories or specific partners) _____

* [ ] Service Providers (List categories or specific providers) _____

* [ ] Law Enforcement (Only if legally required)

* [ ] Other (Specify) _____

Data Security Measures: (Briefly describe how the data is protected)**

* _____

User Rights:**

* [ ] Access to Data: (How can users access their data?)

* [ ] Correction of Data: (How can users correct inaccuracies?)

* [ ] Deletion of Data: (Can users request deletion of their data?)

* [ ] Opt-Out: (How can users opt out of data collection?)

*Percent Daily Values are based on an assumed need for privacy.

Ingredients: Transparency, Control, Clarity, Security

Allergens: Hidden clauses, Legalese, Vague language (These should be avoided)

Keep Data Collection Permissions in a safe place.**Key Improvements and Explanations:**

- **Checkboxes:** Make it easy for users to see exactly what data is being collected.
- **Clear Language:** Avoids jargon and legalese. Uses plain English.
- **Purpose of Collection:** Explains *why* the data is being collected. This is crucial for trust.
- **Data Retention Period:** Specifies how long the data will be kept.
- **Data Sharing:** Clearly identifies who the data will be shared with. Vague terms like "third parties" are replaced with more specific categories.
- **Data Security Measures:** Briefly outlines the steps taken to protect the data.
- **User Rights:** Informs users of their rights regarding their data (access, correction, deletion, opt-out).
- **"Ingredients" and "Allergens":** Uses a playful analogy to highlight the important elements of a good data collection policy.

This "Nutrition Label" approach aims to make data collection permissions more accessible and understandable for everyone. It's a starting point, and the specific details would need to be tailored to the specific data being collected and applicable regulations (like GDPR, CCPA, etc.).