

**BEFORE THE
OFFICE OF SCIENCE AND TECHNOLOGY POLICY**

In the Matter of

**Request for Information On Regulatory
Reform on Artificial Intelligence**

Docket ID No. OSTP-TECH-2025-
0067

**COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION
IN RESPONSE TO THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY ON
REGULATORY REFORM ON ARTIFICIAL INTELLIGENCE**

The Consumer Technology Association® (“CTA”) submits this response to the Office of Science and Technology Policy (“OSTP”) Request for Information on Regulatory Reform on Artificial Intelligence.

CTA’s membership includes over 1200 companies from every facet of the consumer technology industry, including manufacturers, distributors, developers, retailers, and integrators, with startups or small and mid-sized companies being 80 percent of CTA’s members. CTA also owns and produces CES®—the world’s most powerful tech event.

I. INTRODUCTION

CTA applauds the Trump Administration’s (the “Administration”) actions on our nation’s AI policy to remove barriers and maintain American leadership in AI innovation. In this response, CTA identifies existing barriers to the development and adoption of AI technologies and proposes policies for the Administration to remove barriers and facilitate American leadership in AI innovation.

II. RESCIND OUTDATED AI REGULATIONS

Despite President Trump’s AI Action Plan,¹ issued pursuant to Executive Order 14179, Removing Barriers to American Leadership in Artificial Intelligence, there remain outdated agency rules, policies, and guidance specific to AI technologies that are inconsistent with the Trump Administration’s priorities which have not been formally modified or rescinded. These policies either (1) pose unnecessary direct obstacles to AI development and deployment or (2) create regulatory uncertainty posing a barrier to AI innovation due to their ambiguous legal status. We ask OSTP to prioritize modernizing and harmonizing the following to ensure consistency across agencies and provide clear, predictable guidance for responsible AI deployment:

1. **Biden Administration’s Voluntary AI Commitments.**² CTA recommends the Trump Administration formally dissolve or sunset this framework to remove ambiguity about the status of the voluntary commitments.
2. **NIST AI Risk Management Framework (“AI RMF”).**³ Consistent with the AI Action Plan, CTA asks the Administration to revise this framework to reflect the Trump Administration’s AI priorities. Updating this framework is urgent because it is increasingly being referenced in state bills as a de-facto baseline and regulatory anchor.

¹ White House, Winning the Race: America’s AI Action Plan (July 2025), available at <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.

² See White House, Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI (July 21, 2023), available at <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>.

³ National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Jan. 2023), available at <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10>.

3. **NTIA Dual-Use Foundational Models With Open Weights.**⁴ OSTP should evaluate this guidance for consistency with this Administration's AI Action Plan's preference for open weight models.

III. TRADE POLICY

Whether U.S. companies can compete in AI is tied to how they can maintain an edge in technology in the face of global competition, particularly with China. We recommend strong provisions in trade agreements, such as those included in Agreements on Reciprocal Trade ("ARTs"), to address critical issues affecting the competitive landscape for U.S. innovators.

Key areas where ARTs could bolster U.S. AI leadership include:

1. **Trade Barriers:** OSTP should address unfair import tariffs, restrictive import licensing requirements, and discriminatory export control measures. Trade rules should target the growing trend to require disclosure of source code, algorithms and encryption keys as a condition of market access, such disclosures jeopardize intellectual property and undermine fair competition. Further, eliminating discriminatory government procurement policies ensures a level playing field for U.S. companies abroad.
2. **Digital Trade Provisions:** AI leadership requires robust digital trade rules that:
 - a. Oppose tariffs on cross-border data flows, including digital products.

⁴ National Telecommunications and Information Administration (NTIA), Dual-Use Foundation Models with Widely Available Model Weights, NTIA Report (Feb. 2024), available at <https://www.ntia.gov/sites/default/files/publications/ntia-ai-open-model-report.pdf>.

- b. Uphold the World Trade Organization (“WTO”) e-commerce moratorium to prevent governments from imposing customs duties on cross-border data flows.
- c. Prohibit data localization requirements, which fragment the global economy, burden technological operations, and increase security risks.
- d. Ease the free flow of data across borders, ensuring that U.S. innovators remain connected to global supply chains and markets.
- e. Encourage the development of new provisions on trusted technology and AI to align international regulatory frameworks.

Additionally, the Administration should narrow export policies to address legitimate national security concerns without hindering American innovation. This is particularly true in the realm of AI and robotics. In Executive Order 14307 (“Unleashing American Drone Dominance”), for example, President Trump directed agencies to update the export control regulations to promote the export of American-made civil drones to foreign partners. Implementing such directives is critical to ensuring that American technology, including advanced autonomy, remains the gold standard worldwide.⁵

By addressing these trade policy issues, the U.S. can strengthen the global competitiveness of its AI companies and maintain leadership in innovation.

⁵ Exec. Order No. 14307, Unleashing American Drone Dominance, 90 Fed. Reg. 24727 (June 6, 2025), <https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/>.

IV. AMEND THE CHIP SECURITY ACT OF 2025

Enacting the current draft of the Chip Security Act⁶ (“CSA”) would erode trust and endanger the Administration’s vision to diffuse U.S. AI technology. Specifically, burdensome rules on U.S. companies not required for foreign competitors risk incentivizing customers to shift to non-U.S. suppliers, undermining U.S. technology leadership.

The CSA would require chip manufacturers to implement location verification systems within covered products, which creates several logistical and commercial concerns. First, there is no known feasible, real-world location verification solution for AI chips. GPS and network-based methods are easily spoofed, imprecise, and insecure. Location tracking now exists at the system or device level, not embedded within chips themselves. Embedding tracking mechanisms would require dedicated design elements, power sources, and potentially new chips altogether, increasing complexity, costs, and risks of introducing security vulnerabilities.

In addition, embedding location tracking and reporting obligations will likely create unease among international customers concerned about surveillance, driving them away from U.S. chip suppliers. Moreover, mandated location reporting increases risks of exposing sensitive operational data to adversaries, creating new cybersecurity vulnerabilities and potential conflicts with foreign privacy laws.

Before enacting the CSA, CTA urges the following:

1. Direct NIST to work with the private sector to assess feasibility and create standards before imposing mandates.

⁶ See Chip Security Act, H.R. 3447, 119th Cong. (2025), available at <https://www.congress.gov/bill/119th-congress/house-bill/3447/text>.

2. Clarify the scope of the CSA to focus on high-risk items and clearly define terms like “other authorizations.”
3. Align reporting obligations with chip manufacturers who have technical access and include exceptions for allied government customers or operations without connectivity.
4. Define data retention periods and reporting frequency to reduce compliance uncertainty.
5. Extend the implementation deadline to at least two years to allow for standards development and integration of viable solutions.

V. AI AND CYBERSECURITY

AI is transforming cybersecurity by enabling faster threat detection, adaptive defense, and more efficient risk management. However, many federal cybersecurity and data governance frameworks remain fragmented and manual, creating duplicative obligations and unnecessary compliance burdens. Modernizing and harmonizing these frameworks will strengthen resilience, improve coordination across agencies, and allow AI-enabled systems to enhance security at the speed and scale required by today’s threat landscape.

To foster U.S. private sector innovation in AI and address the evolving cyber threat landscape, the Administration should:

1. Collaborate with the private sector to develop guidance and encourage the uptake of recognized standards, ensuring all parties benefit from shared expertise and best practices.

2. Avoid classifying AI systems embedded within cybersecurity solutions as high-risk, to prevent unnecessary regulatory burdens that could hinder development and deployment.
3. Promote the adoption of cybersecurity systems with generative AI (“GenAI”) interfaces and encourage the use of GenAI tools to help mitigate the widespread shortages of skilled cybersecurity professionals.
4. Support mutual recognition of similar certification regimes to reduce duplicative compliance requirements and facilitate cross-border collaboration.
5. Align incident reporting thresholds and disclosure frameworks across federal and state agencies to reflect real-time AI detection capabilities.

As innovators particularly entities subject to the Health Insurance Portability and Accountability Act (“HIPAA”), face duplicate obligations, the Administration is correct to streamline rules. For example, the HIPAA Security Rule (45 C.F.R. Part 164 Subpart C) includes requirements around risk assessments, encryption, and access controls, while the Federal Trade Commission (“FTC”) enforces broad authority over protecting health data under unfair or deceptive practice laws. At the same time, states are enacting new AI-specific cybersecurity mandates, creating a fragmented regulatory environment. **A federal safe harbor framework would alleviate this issue.** Specifically, organizations that align with the NIST AI RMF and Cybersecurity Framework should be deemed compliant for AI governance purposes. This approach would reduce liability risk, incentivize the adoption of best practices, and provide greater regulatory certainty while reinforcing the role of AI in addressing cybersecurity challenges.

VI. PRIVACY AND DATA USE

As the digital economy expands, consumers expect both privacy protection and continued access to innovative, data-driven products and services. Data is used to provide consumers with the products and services that they want, and CTA recognizes that this exchange should be complemented by strong privacy protections. However, the lack of a federal privacy law has created an impediment to innovation.

The U.S. needs a uniform, risk-based, and innovation-friendly federal privacy law to achieve this balance. The absence of a comprehensive federal framework has led to an increasingly complex and fragmented patchwork of state and federal sectoral rules, creating consumer confusion and placing undue compliance burdens on small and medium-sized businesses. A well-structured federal framework that preempts state laws without providing a private right of action would enhance consumer protection while fostering regulatory certainty that spurs American innovation.

Health care privacy regulations present unique challenges that must be addressed to ease new AI-enabled health tools and systems. Laws such as HIPAA govern protected health information collected by covered entities, but they leave gaps when consumer health data falls outside their scope. In response, states like Washington and Nevada have introduced laws to regulate consumer health data not covered under HIPAA. However, this fragmented patchwork of state laws creates compliance complexity for businesses without necessarily enhancing privacy protections.

To address these challenges, any comprehensive federal privacy law should ensure preemption of state laws regulating consumer health data to create a single, uniform regulatory framework. Such a federal law should also include HIPAA-like

safeguards for consumer health AI tools and establish clear, consistent rights for patients nationwide, enabling more efficient compliance and stronger protections for sensitive data.

Federal rules should also be updated to better reflect the capabilities of adaptive AI tools in telehealth, diagnostics, and pharmacy operations. Current regulations, designed around human-led decision-making and static devices, can introduce unnecessary friction when updating AI-driven models for clinical decision support or preventive care. Modernized rules must account for the dynamic nature of AI technologies, allowing for safe, privacy-conscious innovation that enhances patient outcomes without compromising security or care standards.

The Administration should also ensure that aspects of privacy and copyright law developed prior to modern AI technologies do not needlessly burden innovation. As directed by the AI Action Plan, OSTP should support review of FTC final orders, consent decrees, and injunctions - in particular those relying on novel interpretations of Section 5 unfairness authority. For example, broad definitions and restrictions on collection and use of 'sensitive data' that may impede AI training were included in the 2023 Biometric Policy Statement⁷ and 2024 location data enforcement actions against Gravy Analytics & Venntel⁸ and Mobilewalla.⁹

⁷ See FTC, Policy Statement of the Federal Trade Commission on Biometric Information and Section 5 of the Federal Trade Commission Act (May 18, 2023), available at https://www.ftc.gov/system/files/ftc_gov/pdf/p225402biometricpolicystatement.pdf.

⁸ See FTC, Press Release, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites (Dec. 3, 2024), available at <https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers>.

⁹ See FTC, Press Release, FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data (Dec. 3, 2024), available at <https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data>.

In addition, the OSTP could release recommendations on use of privacy-enhancing technologies, such as de-identifying data, creating synthetic data, or otherwise protecting personal data in the AI lifecycle to provide clarity about privacy-protective methods of developing and deploying AI systems.

VII. FEDERAL LEADERSHIP ON AI LAWS

The OSTP should recommend enacting federal laws that would preempt state laws that place conflicting and overburdensome obligations on AI development. In addition to the proliferation of state privacy laws, in 2025 state legislatures have passed laws expanding and fragmenting AI rules, especially when regulating frontier models, automated decisionmaking technologies, employment tools, and commercial chatbots.¹⁰ Conflicting definitions and overlapping, inconsistent requirements are already driving up compliance costs and hindering innovation without proportional risk mitigation, particularly for small- and medium-sized firms that cannot afford to support multiple state differing compliance programs. OSTP can identify areas where lack of uniform, preemptive federal rules are driving a costly and divergent state-by-state approach and to formally call for a moratorium on state AI laws.

While federal leadership is critical, restraint is equally important, particularly with regard to health care. Overregulation of low-risk, administrative AI, such as billing systems or patient scheduling bots, would provide little safety benefit while undermining efficiency gains that reduce provider burnout. Similarly, premature restrictions on generative AI in patient communications could hinder innovation, provided clinicians review outputs or appropriate disclosures are included. In these areas, the

¹⁰ See Multistate, Which AI Bills Were Signed into Law in 2025? (Aug. 8, 2025), available at <https://www.multistate.ai/updates/vol-71>.

Administration should endorse industry-driven best practices, such as those advanced by CTA¹¹, in lieu of rigid federal mandates.

VIII. TRACEABILITY FRAMEWORKS

Federal agencies should adopt performance-based or iterative certification methods for AI-powered traceability tools that demonstrate consistent accuracy and compliance, rather than requiring full re-approval for every algorithmic improvement. This is particularly relevant to the Food and Drug Administration's ("FDA") Requirements for Additional Traceability Records for Certain Foods.¹² Current approval processes were originally designed for static, human-managed systems, and they are ill-suited to the dynamic nature of AI technologies, which continuously learn and improve through algorithmic updates.

AI-powered traceability platforms, such as those employing computer vision and predictive analytics to monitor factors like freshness, contamination risks, and temperature anomalies, require frameworks that accommodate iterative enhancements without triggering revalidation burdens for each update. Present requirements often treat such updates as new system changes, creating delays and excessive re-certification obligations that discourage innovation.

To reduce uncertainty for developers and operators, the FDA should modernize its approach to include flexible certification models for traceability tools while clarifying liability for AI-assisted decisions. Enabling adaptive compliance mechanisms would

¹¹ See e.g. CTA Guiding Principles for the Privacy of Personal Health Data <https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf>.

¹² See Requirements for Additional Traceability Records for Certain Foods, 87 Fed. Reg. 71070 (Nov. 21, 2022), available at <https://www.federalregister.gov/documents/2022/11/21/2022-24417/requirements-for-additional-traceability-records-for-certain-foods>.

promote innovation and accelerate the deployment of AI technologies while safeguarding the transparency and safety of the food supply chain.

IX. LIABILITY FRAMEWORKS

As AI technologies become more integrated into business and consumer applications, existing liability doctrines have not kept pace with the realities of AI-enabled systems. Current frameworks for assigning responsibility are often unclear or fragmented across agencies, creating uncertainty that can slow innovation and adoption. Government can and should clarify liability across the AI value chain—covering developers, deployers, and end users—to provide predictable, fair accountability while supporting responsible advancement and use of AI.

The Administration should update or clarify U.S. liability frameworks to reflect the unique characteristics of AI systems, which differ from traditional products and involve complex interactions among developers, deployers, and users. Liability should apply only when harm is clearly linked to a party's actions and to foreseeable risks within their control, which will promote accountability without discouraging innovation. Additionally, AI liability frameworks should also include safe harbor or affirmative defense provisions for organizations that follow recognized standards and best practices, such as the NIST AI RMF. Clearer standards defining the respective obligations of developers and deployers would give businesses greater confidence in adopting AI tools while maintaining strong consumer protections.

Similarly, the FTC should ensure that its enforcement policies on unfair or deceptive practices recognize these distinctions and focus on intentional misuse or deceptive conduct rather than on good-faith, standards-aligned development and deployment of AI technologies.

X. PERMITTING REFORM

To promote sustainable innovation in modern logistics infrastructure, federal agencies should accelerate permitting for AI-enabled, energy-efficient warehouses and logistics hubs through coordinated approvals and targeted incentives. Federal reforms should ensure that permitting processes balance operational efficiency with equity by guaranteeing that host communities share in the economic benefits while avoiding disproportionate environmental burdens.

We ask the Federal Energy Regulatory Commission (“FERC”), and the Department of the Treasury to streamline regulations and align federal rules for AI-optimized, low-emission warehouse and fleet operations. These next-generation facilities leverage AI to enhance energy efficiency, reduce emissions, and optimize operations. However, delays in permitting processes and fragmented incentives can hinder investment in this critical infrastructure.

The Administration can and should create a streamlined process for federal approvals and incentives to ensure that energy-efficient, AI-enhanced systems are rapidly deployed to cut energy usage and deliver economic and operational benefits to industries and communities alike.

XI. SEMICONDUCTOR POLICY

U.S. semiconductor policy plays a decisive role in shaping the future of U.S. artificial intelligence (AI) development and leadership. To stay competitive, the Administration should prioritize policies that support American semiconductor companies and avoid imposing restrictions that hinder their ability to domestically innovate or manufacture products.

We need to grow the semiconductor value chain to strengthen AI infrastructure. This means expanding the pool of skilled chip designers and adding fabrication facilities to meet the increasing demand for advanced semiconductors.

In addition, investigations on semiconductors conducted pursuant to Section 232 Trade Expansion Act should consider unintended impacts on domestic companies. By creating clear processes for exclusions and duty drawbacks, disruptions can be minimized and continuity in the U.S. semiconductor industry can be assured. These measures, along with a broad focus on developing a resilient semiconductor ecosystem, will safeguard U.S. leadership in AI innovation and technology advancement.

XII. PROMOTE INFRASTRUCTURE DEVELOPMENT

The Administration should promote policies that drive investment in data centers, broadband infrastructure, future-proof network development, and affordable, reliable energy systems. We need these foundational elements to support AI innovation and strengthen the digital economy.

The Administration should prioritize:

1. **Diverse Energy Sources:** Support policies that incentivize private-sector investment in several technologies, while avoiding policies that artificially constrain energy supply.
2. **Modernize the Grid:** Advance policies that promote a modern energy grid and adopt Internet of Things technologies to cut energy waste and improve efficiency.
3. **Expand Data Center Capacity:** Encourage strategic investments in new data center infrastructure and modernize legacy facilities to meet growing computational demands.

4. **Make Networks AI-Ready:** Promote best practices for building networks optimized for AI technologies to ensure scalability, reliability, and security.
5. **Streamline Permitting:** Collaborate with permitting agencies to reduce regulatory bottlenecks for constructing energy facilities, data centers, and broadband infrastructure.
6. **Adopt Energy Efficient Equipment:** Encourage adoption of energy-efficient information and communication technology equipment in data centers to optimize operational performance and efficient energy use.
7. **Balance Cost Sharing:** Ensure that the costs of grid modernization are balanced and promote efficient investment, prevent cross-subsidization, and support reliable, affordable power for all users.

These policies would enable the U.S. private sector to deploy the infrastructure necessary for AI innovation and enhance technological resilience, without unfairly targeting certain users, such as tech companies. Federal investment and regulatory efficiency in these areas are vital for fostering growth and maintaining global leadership in technology.

XIII. WORKFORCE TRAINING PROGRAM ALIGNMENT

The success of AI adoption will depend on the ability of the U.S. workforce to adapt and thrive alongside these technologies. Federal workforce grant, development, and training programs can expand AI jobs and productivity if they prioritize rapid credentialing, digital literacy, and workforce development. As artificial intelligence transforms industries, we need these initiatives to create the AI labor force and ensure the widespread and rapid adoption of AI technologies while building worker trust in AI-

assisted processes. First Lady Melania Trump's leadership in this area is focusing on investment in education is important and is supported by CTA.

To maximize impact, the U.S. Government should collaborate with private sector partners to invest in digital skills training and workforce development programs. Partnerships with industry leaders will align training programs with real-world needs, providing workers with the tools and knowledge necessary to thrive in an AI-driven economy. Modernizing federal workforce initiatives to incorporate AI and digital skill development will help foster economic growth, workforce resilience, and public confidence in emerging technologies.

Federal workforce policy should also modernize pathways for high-skill talent in emerging technologies while investing in broad-based upskilling to strengthen U.S. competitiveness and economic resilience. For example, OSTP should recommend clarifying the requirements of the O-1, EB-1, and EB-2 immigrant visas (reserved for individuals with extraordinary ability or achievement) to explicitly include experts in occupations requiring AI skills, such as AI development, robotics, and quantum computing.

XIV. ADVANCE GLOBAL ALIGNMENT

The Administration should prioritize efforts to promote international alignment of AI regulations to reduce regulatory fragmentation and conflicting compliance obligations. Divergent global frameworks challenges companies operating across borders, increasing costs, uncertainty, and operational friction. Such fragmentation risks slowing innovation and complicating the deployment of AI technologies at scale.

Encouraging mutual recognition of regulatory frameworks with harmonization of international standards, such as ISO42001, promotes responsible innovation and

provides businesses with a clearer path to compliance. We need federal engagement in international regulatory discussions to ensure U.S. companies remain competitive in a global AI economy while mitigating compliance burdens in cross-border operations. In particular, OSTP should support the principle that any mandatory pre-deployment testing should be done by the country where a company is based.

XV. MISCELLANEOUS ISSUES

A. Transportation Innovation and Safety

As OSTP considers barriers to AI-enabled Automated Vehicles (“AVs”), CTA urges the Administration to address the lack of clear federal guidance and the growing patchwork of state-level regulations that create legal uncertainty and hinder innovation and nationwide deployment.

CTA commends DOT Secretary Duffy on his September 2025 announcement to modernize Federal Motor Vehicle Safety Standards (“FMVSS”) for vehicles equipped with automated driving systems (“ADS”).¹³ The proposed modernizations represent a critical step toward aligning safety standards with the operational realities of AVs. CTA suggests NHTSA build on these actions further, to address outdated requirements for manually operated controls and equipment intended only to support a human driver in ADS-dedicated vehicles. CTA also encourages OSTP to review NHTSA’s own publication, FMVSS Considerations for Vehicles With Automated Driving Systems: Volume 1,¹⁴ which identifies multiple FMVSS provisions that pose compliance

¹³ Press Release, Nat’l Highway Traffic Safety Admin., Trump’s Transportation Secretary Sean P. Duffy Advances AV Framework with Plans to Modernize Safety Standards (Sept. 4, 2025), available at <https://www.nhtsa.gov/press-releases/av-framework-plan-modernize-safety-standards>.

¹⁴ Highway Traffic Safety Admin., FMVSS Considerations for Vehicles With Automated Driving Systems: Volume 1, DOT HS 812 796 (Apr. 2020), available at <https://doi.org/10.21949/1530202>.

challenges for AVs—drawing particular attention to standards that should be evaluated within the context of ADSs.

We need continued modernization of FMVSS, coupled with harmonized federal guidance, to unlock the full benefits of AVs, including improved safety, expanded mobility access, and strengthened U.S. leadership in AI-driven transportation.

Further, the Administration should modernize safety regulations governing certain autonomous vehicles and systems to allow cab-mounted warning lights to increase safety. Current Federal Motor Carrier Safety Administration regulations require trucks to alert roadway users when a truck is safely stopped on the side of the road.

Drivers are now required to walk along the shoulder of a busy highway, at times in adverse weather conditions or low light, to place warning triangles behind the truck. The side of the road is an incredibly dangerous place to be. A light-based system removes this exposure to passing traffic, reducing the risk for drivers on the side of the road. Further, a flashing light system could offer faster warning to other motorists when the truck is pulled over, enhancing safety for both the stopped truck and oncoming traffic.

Research shows similar results distinguishing the cab-mounted warning beacons and traditional warning triangles when comparing approaching motorists' abilities to detect, recognize and respond to a stopped commercial motor vehicle, such as changing lanes or slowing down.

Motor carriers operating with a Level 4 ADS were recently granted a waiver by USDOT to use the warning beacons for a limited period under certain conditions and

requirements.¹⁵ This waiver marks a positive step towards a long-term regulatory solution.

After decades of stagnation in innovation in the warning device space, updates to federal rules to allow all trucks to use the proposed light system would show the federal government's support of safety innovation and commitment to improving roadside safety for all roadway users, and further reduce regulatory barriers to expansive deployment of AI solutions across the transportation industry.

B. Healthcare Innovation

When considering the regulation of health AI, the Administration should remember that healthcare is an already highly regulated field and the use of AI in healthcare, while growing quickly, is not new. The FDA has approved more than 1200 AI-enabled medical devices, with the first approved in 1995. However, the Administration should modernize existing healthcare regulations through a risk-based approach to better accommodate AI-enabled tools and workflows.

We need a risk-based approach to regulation to ensure AI developers do not face undue and expensive regulatory burden and can continue to innovate. For example, on December 13, 2023, Dr. Micky Tripathi, National Coordinator for Health Information Technology, Office of the National Coordinator for Health IT ("ONC"), Department of Health and Human Services, testified in front of the House Energy & Commerce Committee that ONC is specifically *not* taking a risk-based approach to requirements for "predictive decision support intervention" AI applications that are supplied by certified health information technology in their Health Data, Technology, and

¹⁵ See U.S. Department of Transportation, Waiver of Warning Device Requirements (Oct. 9, 2025), available at <https://www.fmcsa.dot.gov/safety/carrier-safety/carrier-safety-resources/waiver-warning-device-requirements-effective-october>.

Interoperability HTI-1 Final Rule (45 CFR Part 170).¹⁶ This is directly counter to not only the widely accepted risk-based approach to AI regulation, but it also goes against the risk-based approach to broader health regulation. Additionally, this sets information disclosure requirements for a subset of health AI (AI supplied by certified health IT) that does not align with emerging standards and industry efforts. This could create regulatory fragmentation or duplicative efforts as other frameworks take shape.

Innovative technologies like AI and machine learning continue to transform health care and the ways in which clinicians and patients use data to improve care coordination, diagnostic accuracy, and quality of care. Consumers increasingly want to be active participants in their own care and able to monitor their health and wellness, and share their data with health care providers, applications, caregivers, and family members.

We need a uniform, risk-based, and innovation-friendly federal privacy law to achieve this balance. The absence of a comprehensive federal framework has led to an increasingly complex and fragmented patchwork of state rules, creating consumer confusion and placing undue compliance burdens on small and medium-sized businesses. A well-structured federal framework without a private right of action would enhance consumer protection while fostering regulatory certainty that spurs American innovation.

The FDA should also build on its existing guidance for AI- and machine learning-enabled Software as a Medical Device (“SaMD”) by providing greater clarity on how algorithm-based tools are evaluated. Clear, predictable review standards will help

¹⁶ Statement of Micky Tripathi, Assistant Secretary for Technology Policy, U.S. Dep’t of Health & Human Servs., Before the H. Comm. on Energy & Commerce, 118th Cong. (Dec. 13, 2023), available at <https://www.hhs.gov/about/agencies/asl/testimony/2023/12/13/artificial-intelligence.html>.

developers align early with agency expectations and accelerate access to safe, effective AI-enabled products. FDA should also continue refining its approach to Predetermined Change Control Plans to ensure that regulatory oversight accommodates iterative AI model updates while preserving patient safety.

Finally, the Centers for Medicare & Medicaid Services (“CMS”) should consider how to ensure appropriate adoption of AI and ML tools, as well as other software as a service/SaMD products. Currently, time-based reimbursement codes incentivize inefficient clinician workflows so providers can receive payment. This hurts the adoption of AI innovations, which seek to make health care less expensive and more efficient for clinicians and patients. CMS must consider the impact of AI and ML tools on current valuations and a path forward to ensuring adequate provider reimbursement for tools that will improve patient outcomes and reduce provider burden while still delivering cost savings.

In approving specific digital health product categories for reimbursement, CTA supports the Administration’s statement in the Making America Healthy Again Executive Order that “agencies shall ensure the availability of expanded treatment options and the flexibility for health insurance coverage to provide benefits that support beneficial lifestyle changes and disease prevention.”¹⁷

¹⁷ White House, Presidential Memorandum Establishing the President’s Make America Healthy Again Commission (Feb. 20, 2025), available at <https://www.whitehouse.gov/presidential-actions/2025/02/establishing-the-presidents-make-america-healthy-again-commission/>.

XVI. CONCLUSION

AI is our future. CTA appreciates the Administration's proactive efforts to identify and remove barriers to American leadership in AI innovation. The United States can accomplish President Trump's vision of AI by taking the actions outlined above, laying a foundation for sustained, long-term growth and innovation, ensuring that the U.S. continues to lead in the development of this critical technology.

Respectfully submitted,

CONSUMER TECHNOLOGY ASSOCIATION

By: /s/ J. David Grossman

J. David Grossman
Vice President, Policy & Regulatory
Affairs

/s/ Kerri Haresign

Kerri Haresign
Senior Director, Technology & Standards

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

October 27, 2025