U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

October 27, 2025

Dr. Michael Kratsios
Director
White House Office of Science and Technology Policy
1600 Pennsylvania Avenue
Washington, DC 20500

Re: Response to OSTP's Request for Information on Regulatory Reform for Artificial Intelligence

Dear Director Kratsios:

On behalf of the U.S. Chamber of Commerce ("Chamber"), thank you for the opportunity to respond to the Office of Science and Technology Policy's ("OSTP") Request for Information ("RFI"[1]) on regulatory reform for artificial intelligence ("AI"). This initiative is of critical importance to the business community, and we commend OSTP for its leadership in seeking stakeholder input to shape a forward-looking AI governance framework.

The Chamber strongly supports the recently released AI Action Plan, which we believe offers the necessary "steps to accelerate innovation by fixing a regulatory landscape hobbled by conflicting state-level laws and activist-driven overreach, streamlining permitting for critical AI infrastructure, ensuring reliable and affordable energy for consumers and businesses, and advancing U.S. leadership in AI diplomacy.[2]"

As Vice President Vance aptly stated during February's Artificial Intelligence Action Summit in Paris, "we face the extraordinary prospect of a new industrial revolution... But it will never come to pass if overregulation deters innovators from taking the risks necessary to advance the ball."[3] This sentiment reflects the urgent

[1] United States, Executive Office of the President, Office of Management and Budget. "Notice of Request for Information: Regulatory Reform on Artificial Intelligence." *Federal Register*, 26 Sept. 2025, www.federalregister.gov/documents/2025/09/26/2025-18737/notice-of-request-for-information-regulatory-reform-on-artificial-intelligence.

[2] See U.S. Chamber Statement *available at* https://www.uschamber.com/technology/artificial-intelligence/u-s-chamber-commends-white-house-ai-action-plan

[3] Vance, J.D. "Vice Presidential Pool Reports of February 11, 2025." The American Presidency Project, https://www.presidency.ucsb.edu/documents/vice-presidential-pool-reports-february-11-2025.

need for a regulatory environment that fosters innovation while safeguarding public interest. As noted in the AI Action Plan, the United States needs to establish American AI "as the gold standard for AI worldwide and ensure our allies are building on American technology." It's critical that American AI standards, especially in fields like robotics and other critical technologies, become the gold standard worldwide.

Businesses are experiencing firsthand the transformative impact of AI on American businesses—particularly small enterprises. Our recent report, *Empowering Small Business: The Impact of Technology on U.S. Small Business*[4], highlights a nearly 20% increase in generative AI adoption over the last year, with overall usage nearing 60%. Businesses leveraging AI are experiencing faster growth in sales and hiring compared to their peers, underscoring the technology's role in driving economic vitality.

Studies project that AI could boost U.S. economic growth by 10 to 20% over the next decade.[5] Realizing this potential will require a regulatory framework that is open, adaptive, and aligned with the pace of technological advancement.

In response to OSTP's RFI, we identify challenges created by a growing patchwork of state regulation, and provide detailed input regarding regulatory barriers and opportunities for reform:

I. State Patchwork

One of the most pressing barriers to AI adoption is the current patchwork of differing state AI laws, which disproportionately harms small businesses. The Chamber's *Empowering Small Business* Report found that such entities using AI are doing better in terms of profits and hiring, yet most owners believe that varying state laws—especially those outside their home jurisdiction—will increase compliance costs and litigation risks. This amounts to a tax on Main Street businesses, which now must spend limited resources on lawyers and compliance instead of investing in the growth of their businesses. Many cannot afford such expenses, and these laws further impede their ability to use AI tools that would otherwise reduce both costs and time.

The AI Action Plan rightfully highlights the importance of AI adoption in winning the AI race, stating that "many of America's most critical sectors…. [are] slow to adopt due to a variety of factors, including…. a complex regulatory landscape.[6]"

---

[4] U.S. Chamber of Commerce. Empowering Small Business: The Impact of Technology on U.S. Small Business. (August 2025) *available at* https://www.uschamber.com/assets/documents/Empowering-Small-Business-Report-2025.pdf.

[5] Seydl, Joe, and Jonathan Linden. "How AI Can Boost Productivity and Jump Start Growth." J.P. Morgan Private Bank, July 16, 2024, https://privatebank.jpmorgan.com/latam/en/insights/markets-and-investing/ideas-and-insights/how-ai-can-boost-productivity-and-jump-start-growth.

[6] The White House. *America's AI Action Plan*. The White House, July 2025, www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

With more than 1,100 state bills introduced in 2025, the regulatory action that could follow would create an enormous barrier to AI adoption for American businesses.

For example, a recent report from the Common Sense Institute highlighted the economic impact of Colorado's SB-205, the first comprehensive state AI law enacted. This law will regulate AI use within several sectors including education, employment, financial services, government services, healthcare, housing, insurance and legal services. The report projects that up to 40,000 jobs could be lost[7], and businesses could see a nearly "$7 billion loss in economic output."[8]

Further, we have concerns that laws such as SB-205 would change the standard for discrimination from intent to something more expansive. This concern is shared by Colorado Governor Jared Polis, evident in his signing statement for the bill, which noted that "[l]aws that seek to prevent discrimination generally focus on prohibiting intentional conduct. Notably, this bill deviated from that practice by regulating the results of AI system use, regardless of intent."

As a general matter, discrimination claims involving AI models should require a showing of intent rather than only disparate impact. Requiring a showing of intent—and that the model actually incorporated protected-class information—ensures that liability is tied to culpable conduct rather than mere statistical disparities, which can arise from benign or system-level noise. This threshold preserves space for innovation and legitimate, accuracy-driven model design while focusing enforcement on purposeful or knowing reliance on protected characteristics. By contrast, a disparate-impact-only regime risks over-deterrence and false positives, chilling socially valuable uses of data without meaningfully advancing fairness.

Colorado is not alone. The California Privacy Protection Agency recently finalized a rulemaking taking one line of California's Consumer Privacy Act[9] and turning it into a rule costing businesses half a billion dollars in compliance costs for things like pre-use notifications and algorithmic opt outs.

A patchwork of state-level AI laws creates an unsustainable environment for businesses and hinders U.S. leadership in AI. To avoid this, the Chamber strongly supports a federal strategy that preempts state laws, creating a single, national

[7] Hereford, Caitlin, et al. "Unintended Costs: The Economic Impact of Colorado's AI Policy." Common Sense Institute, 20 Aug. 2025, https://www.commonsenseinstituteus.org/colorado/research/jobs-and-our-economy/unintended-costs-the-economic-impact-of-colorados-ai-policy. Accessed 26 Oct. 2025.
[8] Hereford, Caitlin, et al. "Unintended Costs: The Economic Impact of Colorado's AI Policy." Common Sense Institute, 20 Aug. 2025, https://www.commonsenseinstituteus.org/colorado/research/jobs-and-our-economy/unintended-costs-the-economic-impact-of-colorados-ai-policy. Accessed 26 Oct. 2025.
[9] California Privacy Protection Agency. Text of Regulations: California Consumer Privacy Act Regulations (CCPA Updates, Cyber, Risk, ADMT, and Insurance Regulations). n.d., https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_appr_text.pdf. Accessed 26 Oct. 2025.

standard. While state regulatory roles are appropriate in many contexts such as in the case in insurance, a unified federal approach is necessary for this critical industry.

II. Federal Regulatory Barriers

A. Current Constraints

The Request for Information asks: Which federal statutes and regulations are inhibiting AI deployment in areas such as healthcare diagnostics, autonomous systems, and financial services due to outdated compliance frameworks or a lack of clarity on liability and data usage?

1. Need to address duplicative rules and regulations

To avoid unnecessary bottlenecks in AI adoption, we urge agencies to first review how existing laws already regulate AI. This will help identify and eliminate duplicative rules while clarifying existing frameworks to spur adoption. If this review reveals regulatory gaps, any new rules should be narrowly tailored to address specific, tangible harms and applied consistently across all industry sectors, treating functionally similar AI applications the same regardless of the industry.

2.Trade and Foreign Policy.

Existing U.S. trade and foreign policy frameworks are ill-equipped to address foreign AI regulations that may unfairly target American companies or conflict with U.S. values. We recommend that the Office of Science and Technology Policy (OSTP), in partnership with the United States Trade Representative (USTR), study foreign AI regulatory regimes, particularly those with discriminatory thresholds—like compute capacity or model size—that disproportionately impact U.S. providers. Based on this study, OSTP should identify potential mitigation strategies, including the use of trade negotiations and enforcement mechanisms.

3.Country-of-Origin Uncertainty for AI Models

The AI Action Plan highlights the value of open-source AI while also recognizing the risks from models originating in adversary nations. This creates commercial uncertainty, as potential future restrictions—like domestic preferencing or blocking foreign models—remain unclear. Determining a model's origin is complex because open-source projects often involve global contributors and many variations. Therefore, any regulations in this area must be carefully designed to be practical and avoid unintended consequences.

4.FDA Framework for Software as a Medical Device

While we appreciate the FDA's leadership in regulating AI, the current approach creates uncertainty for healthcare AI developers in a rapidly evolving field. To provide greater clarity, we propose the FDA (1) streamline the process for determining when software falls outside its regulatory scope, and (2) publish updated guidance with examples reflecting modern AI tools and development lifecycles. We also support expanding the use of the Predetermined Change Protocol Plan to better manage emerging technologies.

5. Export Control Policy

The Chamber supports export control policies that are narrowly scoped to address legitimate national security concerns without creating unnecessary disadvantages for U.S. businesses. This is particularly true in the realm of AI, robotics, and other sensitive and emerging technologies. In Executive Order 14307 ("Unleashing American Drone Dominance"), for example, the President directed agencies to update the export control regulations to promote American-made civil drones to foreign partners. Such directives are critical to ensuring that American products, including those built on advanced autonomy, remain competitive worldwide.

We also emphasize the importance of aligning U.S. export control policies with those of trusted trading partners to avoid situations where sensitive technologies are provided to competitors, undermining national security objectives. As the administration contemplates additional tools in relation to AI supply chains, coordination with key allies as well as comprehensive guidance, analyses, and industry engagement will be critical throughout the creation and implementation of any new frameworks.

6. DoD IL4/IL5 Authorization Delays

The Department of Defense's current process for achieving Impact Level 4 and 5 (IL4/IL5) authorizations for software through Defense Information System Agency (DISA) is outdated and inefficient. Vendors face delays of 8 to 12 months to secure approval for cloud products and AI models, limiting the federal government's access to cutting-edge commercial technologies and impeding mission-critical innovation. DISA's policies and manuals have not adapted to security and compliance for AI and continue to deviate from compliance reforms such as FedRAMP 20x.

7. FedRAMP Certification Bottlenecks

The current FedRAMP certification process is a significant barrier to integrating AI features into existing platforms. Adding AI often triggers a full, time-consuming recertification, a procedural rigidity that discourages innovation, hinders new market entrants, and slows the deployment of AI-enhanced solutions. The administration should establish a faster, criteria-based approval path for AI tools,

including the use of temporary FedRAMP and DISA waivers to accelerate delivery to mission users.

8. OMB and GSA Contract Standardization

To accelerate the federal government's adoption of AI, the Office of Management and Budget (OMB) and the General Services Administration (GSA) should implement standardized AI contract terms and conditions. This will streamline procurement, reduce ambiguity, and promote consistency across agencies, ultimately enabling faster and more effective deployment of AI technologies.

9. 21 C.F.R. Part 11 – Electronic Records and Signatures

Promulgated in the late 1990s, Part 11 of the FDA's regulations are misaligned with modern data technologies, and discretionary enforcement has created inconsistent compliance expectations. A better approach would be to repeal outdated provisions and revise the regulation to reflect current best practices for electronic records and signatures, reducing the burden on AI developers.

10. Infrastructure Permitting

The construction of data centers and supporting infrastructure—such as fiber networks, electric grid facilities, and subsea cables—requires multiple permits and approvals across local, state, and federal levels. Current permitting delays increase costs and slow the deployment of critical AI infrastructure. We recommend the Office of Science and Technology Policy (OSTP) work with the Council on Environmental Quality (CEQ) to determine if supplemental guidance or other efforts are needed to streamline infrastructure permitting processes essential to U.S. AI leadership, including:

- Supporting comprehensive permitting reform, consistent with the AI Action Plan, that enhances and expands the power grid to ensure its continued strength while building capacity for future growth.
- Supporting the issuance of a nationwide Clean Water Act Section 404 permit by the U.S. Army Corps of Engineers for data center development, as recommended in the AI Action Plan.
- Improving the Team Telecom review process for submarine cable approvals and directing the National Oceanic and Atmospheric Administration to streamline its subsea cable review procedures.
- Accelerating approval timelines for terrestrial broadband infrastructure on federal lands to support AI-related connectivity needs.

Modernizing Environmental and Historical Preservation Reviews

We also support the Federal Communications Commission's (FCC) efforts to modernize its National Environmental Policy Act (NEPA) rules in alignment with recent CEQ guidance and federal reforms. The Fiscal Responsibility Act of 2023 clarified NEPA thresholds and deadlines, while Executive Order 14154 directed agencies to prioritize efficiency. In this context, the FCC's proposed updates—such as expanding categorical exclusions and narrowing the scope of review—are timely and necessary to accelerate AI infrastructure deployment while maintaining environmental safeguards.

To fully realize these goals, the National Historic Preservation Act (NHPA) rules must be updated in parallel. We urge the Commission to clarify that projects without "substantial Federal control and responsibility" are not federal undertakings under Section 106 of the NHPA. Procedures should be aligned accordingly, with clear, enforceable consultation timelines for State Historic Preservation Offices and Tribal Nations.

Accelerating Fiber Deployment on Federal Lands

Fiber deployment across federal lands is frequently delayed by complex permitting processes involving the U.S. Forest Service, the Bureau of Land Management, and the National Park Service. As data centers become more regional, these challenges will become more acute. We recommend OSTP work with these agencies to streamline permitting procedures for broadband infrastructure on federal lands, consistent with the AI Action Plan's emphasis on accelerating the deployment of foundational infrastructure.

11. Financial Services Regulatory Barriers

The ability of financial institutions to deploy advanced AI models for fraud detection, credit risk assessment, and compliance monitoring is significantly constrained by conflicting and outdated regulatory frameworks. For instance, ambiguity in federal model risk management guidance issued by the Office of the Comptroller of the Currency ("OCC"), Federal Reserve Board ("FRB"), and Federal Deposit Insurance Corporation ("FDIC") has slowed the adoption of innovative AI/ML models. Additionally, data privacy statutes such as the Gramm–Leach–Bliley Act ("GLBA"), combined with varying state-level laws, create substantial barriers to using customer data for AI training—limiting the effectiveness of AI-driven solutions. Restrictions on cross-border data flows further inhibit collaboration and innovation in global AI projects. Addressing these regulatory challenges would enable more robust and responsible AI deployment in financial services, enhancing security, compliance, and customer experience.

12. Autonomous Vehicles

AI enables autonomous vehicles (AVs) to perceive the world around them, safely navigate roads, and make real-time decisions. Removing barriers to the deployment of AI in AVs will help improve road safety, increase mobility, and support U.S. leadership in this technology. The National Highway Traffic Safety Administration (NHTSA), under this Administration, has prioritized U.S. leadership and encouraged the commercial deployment of AVs by taking steps to modernize vehicle standards to account for AI. We support NHTSA's continued work and recommend removing requirements for manually operated controls and equipment intended only for a human driver in level 4 and level 5 AVs.

13. Workforce and Immigration (USCIS, State Department)

Current immigration pathways do not adequately reflect the evolving needs of the AI workforce. To sustain U.S. leadership in AI, it is critical to attract and retain top global talent in fields such as AI development, robotics, and quantum computing. We recommend OSTP support the clarification of eligibility criteria for high-skill visa categories—including O-1, EB-1, H-1B, and EB-2—to explicitly recognize individuals with expertise in AI-related disciplines. Clearer guidance would reduce uncertainty for applicants and adjudicators, streamline processing, and ensure the U.S. remains competitive in the global race for AI talent.

B. Specific Regulatory Barriers

The Request for Information asks: Which regulations and federal laws—including those related to privacy, procurement, and licensing—require modernization to accommodate AI capabilities?

1. DoD Cloud Computing Security Requirements Guide (CC SRG)

The existing Cloud Computing Security Requirements Guide (CC SRG) framework, while critical for ensuring security, imposes lengthy and rigid processes that slow down the authorization of AI-enabled cloud services. These delays hinder timely access to advanced technologies for defense and civilian agencies. We recommend DISA revise the SRG to take advantage of National Institute of Standards and Technology (NIST)-authored AI overlays and treat software-as-a-service tools differently than other technology lower in the stack.

2. DoD Risk Management Framework (RMF)

The RMF's static, manual-heavy approach is incompatible with dynamic AI systems. The framework requires modernization to enable continuous authorization and monitoring that reflects the real-time nature of AI operations.

3. Red Teaming for AI Safety (18 U.S.C. §§ 2258A, 2258E; Export Control Regulations).

Current U.S. criminal statutes prohibiting the creation and dissemination of child sexual abuse material (CSAM) and obscenity may inadvertently restrict legitimate safety research aimed at preventing harmful outputs. We recommend creating narrowly tailored exemptions that permit red teaming for the purpose of reducing the proliferation of online child sexual exploitation or preventing the online sexual exploitation of children, subject to appropriate governance protocols.

4. E-Labeling Regulations (21 C.F.R. §§ 201.100, 201.100(d), 201.57(c)(18) & (d))

Current FDA interpretations require manufacturers to provide paper copies of prescribing information with promotional labeling. This requirement is outdated and inefficient, especially when electronic versions are more accurate and accessible. Modernizing these rules would reduce costs and improve information delivery.

5. Medication Guide Distribution (21 C.F.R. §§ 208.24(b), (c), and (e))

The regulation's requirement for direct paper distribution of Medication Guides is unnecessarily burdensome. Explicitly permitting electronic distribution would streamline compliance and enhance patient access to up-to-date information.

6. Paragraph IV Notices (21 C.F.R. §§ 314.52; 314.95)

The current system presumes hard copy delivery of Paragraph IV notices to FDA for approval of generic drugs, which is inefficient and inconsistent with modern communication practices. Transitioning to a fully electronic system would improve transparency and reduce administrative overhead.

7. Credit Underwriting Constraints

The Equal Credit Opportunity Act ("ECOA") requires lenders to provide specific reasons for adverse credit decisions, which limits the use of complex AI models that cannot produce easily interpretable outputs. This restricts innovation in credit scoring and underwriting. ECOA's notice requirement makes it difficult to use advanced AI models, as it constrains both the data inputs and the explanations that can be provided to consumers. Creating an "explainability safe harbor" would allow institutions to use modern AI underwriting tools under internal governance systems while still meeting ECOA's transparency requirements.

8. Model Risk Management Guidance

Federal guidance under 12 U.S.C. § 1818 and § 1831p-1—including FRB SR 11-7 and OCC Bulletins—acts as de facto regulation for banks but has not kept pace with AI innovation. It treats all models uniformly, requiring extensive documentation and oversight, even for low-risk AI tools. This slows deployment, increases costs, and

discourages iterative improvements. Outdated guidance imposes high compliance burdens, deterring fintech partnerships and limiting banks' access to modern AI solutions. Safe harbor provisions or carveouts for lower-risk models—through updated regulatory guidance—would reduce friction and support responsible AI adoption.

9. GLBA Data Use Restrictions

GLBA (15 U.S.C. §§ 6801–6809), along with CFPB Regulation P and SEC Regulation SP, imposes strict limitations on the use and sharing of nonpublic personal information. These constraints hinder the use of customer data for training AI models, particularly when outsourcing to cloud providers is interpreted as "sharing," triggering opt-out requirements. Compliance reviews to confirm statutory exceptions or obtain consent are often lengthy, delaying deployment of AI solutions. GLBA's restrictions on data sharing and reuse create significant obstacles for AI development, especially in financial services where access to high-quality customer data is essential. Clarifying permissible uses of anonymized data and issuing updated compliance guidance would facilitate responsible AI deployment. Explicit exceptions for fraud prevention and security applications would also support cross-institutional collaboration to combat financial crime.

10. Anti-Fraud and Anti-Money Laundering (AML) Limitations

Under the Bank Secrecy Act (31 U.S.C. § 5318(g); 12 C.F.R. § 21.11), current regulations require that suspicious activity reports (SARs) be reviewed and filed by humans. There is no clear regulatory permission—or prohibition—for fully automated SAR filings. This ambiguity, combined with model-risk expectations, limits the use of AI in real-time anomaly detection and network-based money laundering identification. Manual SAR review requirements and unclear guidance on automation hinder the deployment of AI tools for financial crime prevention, reducing speed and accuracy in detecting illicit activity. Regulators should permit carefully controlled AI-driven SAR decisions or expedited pilot programs for low-risk models. This would enable financial institutions to leverage AI for faster, more effective fraud detection while maintaining appropriate oversight.

11. Underutilized Administrative Tools:

The Request for Information poses the following question: Underutilized Administrative Tools: Waivers, exemptions, and experimental authorities exist but are inconsistently applied or difficult to access. How can greater use of these tools enable safe, controlled experimentation with AI technologies?

C. Limited Use of Waivers and Exemptions

Agencies possess the authority to grant waivers or exemptions for innovative technologies, yet these tools are rarely used in the AI context. Expanding their application could accelerate pilot programs and reduce unnecessary delays.

1. Experimental Authorities

Mechanisms that allow for controlled testing of new technologies are underutilized. Greater use of experimental authorities would enable agencies to evaluate AI solutions in real-world settings without full regulatory burdens.

D. Structural Incompatibilities

The RFI observes that some regulatory regimes are fundamentally misaligned with the operational models of AI. Accordingly, it seeks input on which targeted statutory amendments are necessary to preserve core regulatory objectives while still permitting the lawful deployment of AI.

1. Lack of AI-Specific Security Control Overlays

Existing security frameworks (e.g., FedRAMP, DoD CC SRG, NIST SP 800-53) are designed for traditional IT systems and lack overlays tailored to AI. Requiring cloud service providers to implement automated, auditable evidence of AI-specific controls—such as Assured Workloads monitoring—would align with modernization efforts like FedRAMP 20x and reduce manual compliance burdens.

2. Static Authorization Models

Traditional federal agency Authority to Operate (ATO) processes, which allow systems to operate in a federal environment, rely on static assessments that are incompatible with the dynamic nature of AI systems. Transitioning to continuous AI system and model authorization would better reflect real-time operations and reduce unnecessary delays. Federal agencies should move from a point-in-time compliance framework to a continuous monitoring posture to assess risk more efficiently and take advantage of commercial solutions.

3. Privacy Regulation Updates

The Department of Health and Human Services should modernize privacy regulations, including the rules under the Health Insurance Portability and Accountability Act (HIPAA), to enable responsible data use for AI training. Clear safeguards and guidance would support innovation while maintaining strong consumer protections.

E. Need for Clarification

The Request for Information notes the uncertainty caused by ambiguous rules and asks what specific guidance, interpretive rules, or standards are most needed to provide clarity for developers and users.

1. Security and Authorization Guidance

AI-specific overlays or interpretive guidance should be issued to map AI concepts to established security controls. Current frameworks are written for traditional IT and do not adequately address AI-specific concerns related to data, models, and ModelOps.

2. Data Provenance and Quality Controls

To ensure the integrity and traceability of AI training data—especially in sensitive environments governed by IL4/IL5 CUI standards—clear, auditable control statements are essential. We also emphasize the value of a voluntary, open, and multistakeholder approach to building trust and ensuring compliance. This collaborative model supports innovation while maintaining high standards for data governance and accountability.

3. Continuous Monitoring vs. Reauthorization

Clear criteria should be established to determine when an operational AI model requires a new Authority to Operate (ATO) versus when continuous monitoring is sufficient. This would resolve conflicts between static authorization models and dynamic AI deployments.

4. Isolation and Segmentation Requirements

Minimum physical, logical, and cryptographic separation controls should be defined for AI components—such as models and CUI data—within multi-tenant IL5 environments. This would enhance security without imposing impractical burdens.

5. NIST SP 800-171 / CNSSI 1253

While these standards provide a critical foundation for cybersecurity, they currently lack clear guidance on the implementation of AI-specific controls. We emphasize the need for additional, targeted direction to address this gap, as the existing ambiguity contributes to compliance uncertainty and delays in adoption.

6. Rule 56 Duty of Disclosure and AI

The requirements under 37 CFR 1.56 of the USPTO for citing prior art do not neatly apply to AI-generated outputs. Developers may struggle to cite AI-generated insights, especially when the underlying references are unclear or uncitable. Courts

should consider evaluating Rule 56 obligations to avoid unnecessary delays and excessive citation burdens.

7. Clarifying Regulatory Expectations

Federal regulators should issue interpretive guidance or initiate notice-and-comment rulemaking to provide clarity on the use of artificial intelligence AI within sectors such as financial services. Clear expectations would reduce uncertainty and support responsible innovation.

8. Need to Address Legacy Frameworks

Numerous legacy rules, policies, and guidance documents related to AI development, use, and enforcement remain in effect and have not been formally modified or rescinded. These frameworks are often inconsistent with the Trump Administration's AI Action Plan and stated priorities. Their continued application may (1) impose unnecessary regulatory burdens on AI development and deployment or (2) create legal uncertainty due to their ambiguous status. We recommend OSTP evaluate these frameworks and issue recommendations for their revision or formal rescission to ensure alignment with current federal AI policy:

- Biden Administration Voluntary AI Commitments (Sept. 2023). We recommend formally dissolving or sunsetting this framework to eliminate ambiguity regarding its enforceability and relevance under the current policy direction.
- NIST AI Risk Management Framework 100-1 (Jan. 2023). We recommend revision to align with the AI Action Plan. Notably, this framework is increasingly cited in state legislation as a de facto regulatory baseline, which may inadvertently entrench conflicting standards.
- Department of Justice Criminal Division Evaluation of Corporate Compliance Programs (Sept. 2024). AI risk management is treated as a specific factor in prosecutorial decision-making. We recommend clarification or revision to ensure consistency with a risk-based, innovation-friendly approach.
- Department of Labor Artificial Intelligence and Worker Well-Being: Principles and Best Practices for Developers and Employers (Oct. 2024). Although removed from the Department's website, the formal status of this guidance remains unclear. Recommend OSTP confirm its rescission or provide updated guidance consistent with the AI Action Plan.
- NTIA Report on Dual-Use Foundational Models with Open Weights (July 30, 2024). This report should be evaluated for consistency with the

AI Action Plan's stated preference for open-weight models. Clarification is needed to ensure that federal policy does not inadvertently discourage open innovation or impose conflicting expectations on developers.

9. Streamlining Interagency Coordination and Oversight

Regulatory responsibility for AI is fragmented across multiple agencies, leading to inconsistent interpretations, duplicative requirements, and a lack of clear, harmonized expectations. To improve efficiency and clarity, the administration should streamline interagency processes and establish centralized coordination mechanisms. Developing joint statements and common definitional frameworks would further harmonize expectations and improve consistency in AI oversight. Additionally, we call for greater transparency in how agencies use AI and manage data.

10. Resource Limitations

Many agencies lack the technical expertise and staffing needed to evaluate and authorize AI systems promptly. Increased investment in AI-specific regulatory capacity is essential to keep pace with innovation and ensure timely access to advanced technologies. We also highlight the importance of sustained and additional research funding to help spur further innovation and AI adoption.

III. Conclusion

The Chamber commends OSTP for its leadership in advancing a national strategy for AI and appreciates the opportunity to provide input on needed regulatory reform. As outlined in this response, the current regulatory landscape—marked by fragmented state laws, outdated federal frameworks, and procedural bottlenecks—poses significant barriers to AI adoption, particularly for small businesses and critical sectors like healthcare, defense, and financial services. To ensure the United States remains the global leader in AI innovation, federal action must prioritize clarity, consistency, and modernization. This includes harmonizing standards across agencies, streamlining approval processes, enabling responsible data use, and adopting risk-based approaches to oversight.

By removing unnecessary burdens, accelerating the permitting of supportive infrastructure, and enabling practical deployment, the Administration can unlock AI's full potential to drive economic growth, strengthen national security, and improve the lives of American consumers. The Chamber stands ready to partner with OSTP and other federal stakeholders to build a regulatory environment that fosters innovation, protects the public interest, and secures U.S. leadership in the AI era.

Sincerely,

Michael Richards
Executive Director
Chamber Technology Engagement Center
U.S. Chamber of Commerce