

2/21/2025 via FDMS with attachment

Paulo Carvao

See attached file(s) The Dynamic Governance Model advocates for an incremental, iterative process with a responsive system of standards, audits, and compliance frameworks that adapt over time. The model fosters an environment where government oversight complements industry expertise and acknowledges that today's pace of innovation requires a regulatory framework capable of evolving alongside technological advancements. It has three core components: a. Public-private partnerships for the creation of evaluation standards. b. A market-based solution for audit and compliance. c. A system of accountability and liabilities set by legislatures, existing executive agencies, and the courts.

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

### Introducing the Dynamic Governance Model for AI in the United States

<https://www.hks.harvard.edu/centers/mrcbg/publications/awp/awp251>

**Paulo Carvão** is a Senior Fellow at Harvard Kennedy School’s Mossavar-Rahmani Center for Business and Government, specializing in Tech Policy and AI regulation. He is a former IBM executive with three decades of experience in digital transformation, cloud, and AI integration. Currently an advisor to tech startups and a venture capital investor, Paulo has held fellowships at Harvard’s Advanced Leadership Initiative and Safra Center for Ethics. He serves as the inaugural Entrepreneur-in-Residence at the Harvard Kennedy School’s GovLab.

**Slavina Ancheva** is a Harvard Kennedy School Master in Public Policy candidate and a Fulbright Scholar. She is a research assistant for Senior Fellow Paulo Carvão at the Mossavar-Rahmani Center for Business and Government. Before the Kennedy School, Slavina worked in the European Parliament as a Policy Adviser and Head of Office for one of the leading negotiators on the EU’s Artificial Intelligence Act, the world’s first comprehensive law on AI.

**Yam Atir** is a Harvard Kennedy School Master in Public Administration candidate. She is a research assistant to Senior Fellow Paulo Carvão at the Mossavar-Rahmani Center for Business and Government. Before attending the Kennedy School, Yam co-founded and led a tech policy think tank, focusing on macro-level research on technology ecosystems and providing strategic advice on global government-tech relations and emerging technology policies.

==== x ====

As the discussion of artificial intelligence regulation continues to evolve, policymakers face a dilemma: How can one foster innovation while ensuring safety, fairness, and societal well-being? The answer lies in a balanced approach - a dynamic model capable of evolving with technology. We propose an extra-regulatory framework<sup>1</sup> rooted in public-private collaboration, where regulatory clarity and accountability mechanisms are co-developed by government and industry.

The [Dynamic Governance Model](#) advocates for an incremental, iterative process with a responsive system of standards, audits, and compliance frameworks that adapt over time. The model fosters an environment where government oversight complements industry expertise and acknowledges that today’s pace of innovation requires a regulatory framework capable of evolving alongside technological advancements. It has three core components:

- a. Public-private partnerships for the creation of evaluation standards.
- b. A market-based solution for audit and compliance.
- c. A system of accountability and liabilities set by legislatures, existing executive agencies, and the courts.

---

<sup>1</sup> A word on the term “extra-regulatory framework”: This work does not advocate for any specific legislation or statute to regulate the technology. The focus, instead, is on a method that can be applied to different policy objectives, from smaller, niche-based policies to larger AI national policy initiatives.

## **RFI on the Development of an AI Action Plan – The Dynamic Governance Mod**

A Notice by the National Science Foundation on 02/06/2025

### **A New Governance Model**

The rapid adoption of artificial intelligence and its role as a transformative general-purpose technology has brought the United States to a pivotal moment. While the country has historically embraced innovation with a light regulatory touch, AI advancement's unique pace and scale demand a recalibration of this approach. The challenge is clear: How can we maintain the dynamism of technological progress while ensuring AI's safe, ethical, and equitable deployment? Addressing this challenge requires a new governance model that balances innovation with regulation, fosters collaboration between public and private sectors, and builds public trust in the potential of AI.

The American system, while imperfect, has consistently demonstrated its ability to drive technological and economic growth. This system, rooted in a combination of entrepreneurial spirit, public and private investment, and an open market, has fostered innovation across industries. From the early days of the Industrial Revolution to the rise of the Internet and modern digital technologies, the U.S. has maintained its leadership by balancing economic incentives with strategic policy interventions. Innovation has been a crucial driver of American economic growth and contributed as much as half of the nation's economic growth in the 20th century. This technological progress has led to new industries, products, and services that have fundamentally transformed the American economy and improved living standards. (The White House, 1995) The information technology (IT) sector has been a powerful driver of economic growth in recent decades, with an outsized contribution to the U.S. economy, creating high-paying jobs, driving exports, and spurring innovation across various sectors. (Atkinson, 2022)

Like previous general-purpose technologies such as electricity and the Internet, AI could reshape industries, create new opportunities, and enhance the quality of life. A growing consensus among policymakers, industry leaders, and academics is that safeguards are essential to ensure AI applications' safe and ethical deployment. These safeguards aim to build public trust and minimize harm, yet the specifics of their implementation remain a matter of debate.

Technological innovation and legislation operate on fundamentally different timelines. Innovation often occurs rapidly and unpredictably, driven by breakthroughs, market dynamics, and entrepreneurial experimentation. By contrast, the legislative process is slow and intentionally designed to ensure thorough deliberation, consensus-building, and stability. This inherent disparity creates challenges in regulating fast-moving technologies like AI, where static regulatory frameworks can struggle to keep pace with the speed of development and deployment. The rapid evolution of AI demands a dynamic approach to governance that allows for adaptability and continuous refinement while preserving the measured oversight required to safeguard public interests.

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

A strictly ex-post approach to regulating AI, relying solely on antitrust actions and litigation, is insufficient to address this technology's unique challenges and potential for catastrophic risks. While antitrust enforcement and legal recourse play a vital role in correcting abuses and ensuring accountability, they are inherently reactive. Such mechanisms often come into effect only after harm has occurred, making them ill-suited to prevent high stakes risks like safety failures, systemic biases, or widespread societal disruption. Moreover, the complexity and pace of AI innovation can outstrip the ability of courts and regulators to respond effectively. At the same time, ex-ante regulation, while proactive, has its limitations. Static regulatory frameworks can struggle to keep up with rapid and unpredictable technological innovation, risking either obsolescence or overreach that stifles progress.

These phenomena underscore the need for a dynamic regulatory approach that combines the foresight of ex-ante measures with the adaptability to evolve alongside technological advancements. Such a system would complement existing ex-post mechanisms, creating a comprehensive framework to promote innovation and accountability. A well-crafted tech policy and regulatory framework must act as both an enabler and a safeguard, incentivizing the development of technologies that address existing limitations while ensuring accountability and public trust. By embracing a dynamic and collaborative approach to regulation, incorporating public-private partnerships, and ongoing dialogue, policymakers can create an ecosystem where safety and innovation coexist.

Evolution in the governance of AI is needed, leveraging the strengths of both industry and government. Industry brings technical expertise, innovation capacity, and real-time insights into technological trends, while the government safeguards public interests through oversight, accountability, and policy direction. By integrating these complementary roles, such a scheme can adapt to the rapid pace of AI advancements, allowing regulatory frameworks to evolve with technological developments.

To address the challenges and opportunities presented by artificial intelligence, we propose a **Dynamic Governance Model** centered on structured collaboration between government and industry. At the heart of this model is an entity tasked with setting clear standards in partnership with the private sector. These public-private partnerships would go beyond mere consultation, fostering active collaboration in developing, implementing, and iterating on policies that align innovation with societal priorities. A key feature of this model is the incorporation of commitments by industry players underpinned by a robust accountability scheme, including clear delineation of liability and mechanisms for independent audits.

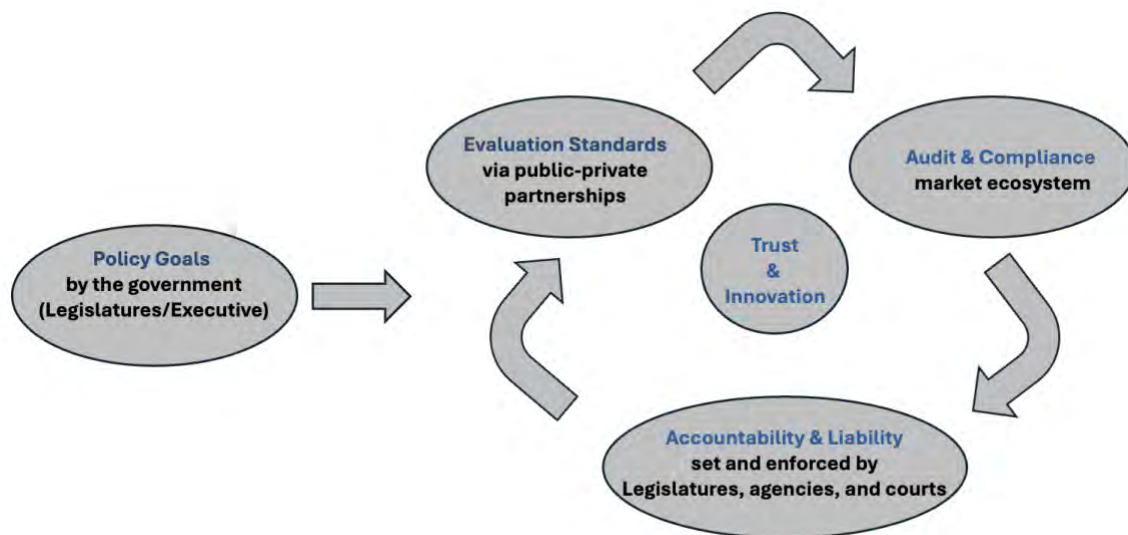
The extra-regulatory model is designed to be modular, light, and of general application. The modular nature of the model allows it to be implemented in phases, starting from different entry

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

points. It is light enough to be built on top of and complement existing legislation and judicial frameworks, reducing the implementation burden on Congress and the industry ecosystem. Its general applicability allows policymakers to decide what use cases to prioritize (a risk-based approach, sectoral phased implementation, focus on larger companies, and gatekeepers are examples of policymaking and political decisions that can be made at implementation time).

This proposal requires decisive congressional action, including a review and potential expansion of statutory authorities to support the framework. By enacting clear policies, Congress can enable adaptive regulation that steers AI innovation in a safe direction and safeguards the nation's leadership in this critical enabling technology. This balanced approach ensures that while AI's transformative potential is fully realized, its deployment remains aligned with ethical standards and public trust.



### The Dynamic Governance

The Dynamic Governance Model begins with an essential role for the government: setting clear policy goals. These goals should balance innovation with the public interest, ensuring that AI systems contribute positively to economic growth while safeguarding societal values. With these goals established, the model is made of three interconnected steps. First, Evaluation Standards are set via public-private partnerships that reflect technological feasibility, policy goals, and societal priorities. These standards create a benchmark for responsible AI development and deployment. Second, a market ecosystem for audits and compliance must be created, wherein independent entities assess adherence to the established standards. The process of audits and compliance ensures that AI systems are safe and ethical and meet transparency and reliability requirements. Finally, a robust system of accountability and liability must be codified and enforced by legislatures, regulatory agencies, and courts. Together, these components form a

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

closed feedback loop where the insights gained from implementation, compliance monitoring, and enforcement inform the continuous improvement of the evaluation standards. With active participation from the government, industry, and civil society, we embed trust into this cycle. The dynamic model ensures adaptive governance that evolves alongside technological advancements. We will now look at the details for each step.

### Evaluation standards

The success of the Dynamic Governance Model hinges on establishing robust and adaptive evaluation standards. These standards must be developed through collaborative public-private partnerships that draw on the expertise of industry leaders, academic researchers, policymakers, and civil society organizations. Existing models, such as the U.S. Artificial Intelligence Safety Institute (AIS) under NIST, provide a framework for AI safety and risk management. However, as the NTIA Accountability Report points out, these efforts often lack enforcement power and standardized methodologies for independent evaluations. (NTIA, 2024) Public-private partnerships should set actionable, measurable, and enforceable standards to address this gap.

Importantly, evaluation standards should encompass technical and non-technical dimensions of AI accountability and reflect technological feasibility, ethical considerations, and societal values. The implementation of evaluation standards requires a flexible, iterative approach that can accommodate technological evolution. While this work does not aim to provide a fully developed implementation plan, we recommend several key steps. First, as suggested by the NTIA, a structured public-private dialogue platform could be formalized to ensure ongoing collaboration in updating standards. This platform would allow the sharing of best practices, emerging risks, and lessons learned from real-world applications. One attempt at creating such a platform is the “Promoting United States Leadership in Standards Act of 2024,” introduced in December 2024 – **U.S. Congress: H.R. 10281, 118th Cong. (2024)**. A bipartisan effort by the Senate, also in December 2024, introduced “A bill to establish the Artificial Intelligence Safety Review Office in the Department of Commerce, and for other purposes” – **U.S. Congress: S. 5616, 118th Cong. (2024)** (Nihill, 2024). These examples demonstrate Congress’s efforts to codify initiatives originally established through executive orders. Supreme Court decisions that limit agency discretion make incorporating these initiatives into statutory language critically important.

Second, pilot programs should be launched in sectors where AI adoption presents significant risks and opportunities, such as healthcare, finance, and critical infrastructure. These pilots would provide crucial feedback on the practical implementation of Evaluation Standards and inform their refinement.

Finally, the NTIA report highlights the importance of developing and certifying independent evaluators and auditors to foster consistency and trust. While audits and compliance will be

## **RFI on the Development of an AI Action Plan – The Dynamic Governance Mod**

A Notice by the National Science Foundation on 02/06/2025

discussed in the next section, evaluation standards must be directly tied to these downstream accountability mechanisms. Only through regular, independent evaluation can these standards remain relevant and effective in mitigating risks while fostering innovation.

A valid criticism of a public-private partnership for setting evaluation standards is the risk of regulatory capture by powerful industry actors. Several strategies can be employed to mitigate this risk. First, ensuring balanced stakeholder representation by including diverse groups such as civil society, academia, consumer advocates, and smaller businesses reduces the risk of dominance by a few large players. Second, establishing independent oversight mechanisms—such as third-party audit bodies—enhances impartiality in enforcement. The following section will cover the oversight mechanisms in more detail. Transparency is critical, with public consultations and mandatory disclosure of interactions between regulators and industry representatives fostering trust. Robust conflict-of-interest policies, including cooling-off periods for regulators transitioning to industry, help limit undue influence. Legislative oversight, judicial review, and use of decentralized standards-setting bodies, such as NIST or IEEE (Institute of Electrical and Electronics Engineers), can further prevent regulatory capture by distributing decision-making authority. Adopting performance-based regulations, which focus on outcomes rather than prescriptive rules, limits industry influence over specific technical requirements. Finally, periodic reviews and sunset clauses ensure that policies remain relevant and effective over time.

### **A market ecosystem for audits and compliance**

Creating a robust market ecosystem for audits and compliance will be a key improvement over current voluntary commitments, which, while valuable, often lack enforcement mechanisms and consistency. (The White House, 2023) To build an effective ecosystem, one can draw lessons from other well-established industry-led compliance frameworks.

A relevant example is UL (Underwriters Laboratories), one of the largest and oldest independent safety science companies. (Kagan, 2023) For over a century, UL has set industry benchmarks for product safety, certifying products ranging from consumer electronics to medical devices. Its model demonstrates how an independent, industry-recognized certification body can enhance safety, build trust, and facilitate market access. The UL illustrates how structured, industry-wide compliance mechanisms can contribute to market trust and safety, enabling innovation and competition.

There are also significant parallels to be drawn from accounting standards. Systems like U.S. GAAP (Generally Accepted Accounting Principles) and IFRS (International Financial Reporting Standards) have established a common framework for financial reporting across industries and countries. The Securities and Exchange Commission (SEC) acts as one of the regulatory bodies

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

overseeing the standards and mandates transparency through extensive disclosures and regular audits. This approach ensures that financial information is reliable and comparable, fostering trust in financial markets. Significantly, accounting standards are periodically revised to reflect changes in business environments, demonstrating the need for iterative updates to standards as technology evolves. GAAP and IFRS face ongoing criticisms regarding their complexity, potential for manipulation, and ability to reflect a company's financial position accurately. However, it would be hard to imagine a world without accounting standards and the associated economic chaos, reduced transparency, impact on business operations, and impeded global financial cooperation and development.

In much the same way, a market ecosystem for AI audits and compliance requires standardized evaluation protocols, clear regulatory oversight, and mechanisms to ensure that standards evolve. The standardization, compliance, transparency, and continuous improvement principles underpin product certification and financial reporting frameworks and offer a blueprint for creating a similar ecosystem in the AI space.

The following steps can be considered for establishing this ecosystem:

1. **Standardized Audit Criteria:** Like evaluation standards, public-private partnerships should define standardized criteria for AI audits, specifying what aspects of an AI system (e.g., safety, fairness, privacy, transparency) must be evaluated and how. These criteria should be publicly accessible and regularly updated to reflect technological advancements and emerging risks.
2. **Certification and Oversight Bodies:** Independent certification bodies, like UL or financial accounting firms, should be established to conduct audits. These bodies would be responsible for certifying AI systems against the established standards. Sectoral regulatory agencies could oversee these bodies, ensuring accountability and adherence to auditing protocols.
3. **Auditor Qualification and Certification:** To ensure high-quality audits, auditors must be certified based on clear qualifications and expertise in the technical and ethical aspects of AI. A national auditor training and certification program could be launched in collaboration with universities and industry partners.
4. **Mandated Disclosures and Reporting:** As with financial reporting, companies deploying high-risk AI systems should be required to disclose key information about their systems' design, testing, and deployment. Standardized disclosure formats, such as model cards and datasheets, would enhance transparency and enable stakeholders to assess compliance more effectively.
5. **Sector-Specific Pilots:** Pilot programs could be launched in high-risk sectors (e.g., healthcare, finance, autonomous vehicles) to test the feasibility of audit protocols and

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

identify best practices for implementation. Insights from these pilots would inform the broader rollout of audit requirements across industries.

6. **Iterative Updates:** Just as accounting standards are regularly revised, AI audit criteria should be updated based on feedback from auditors, regulators, and industry stakeholders. This iterative process will ensure that standards remain relevant and robust in the face of rapid technological change.
7. **Federal Support for the Ecosystem:** Federal agencies should provide programmatic support to accelerate the development of a vibrant market for AI audits. This support includes funding research on auditing methodologies, developing technical audit infrastructure, and facilitating public-private partnerships. Additionally, federal procurement rules could require government suppliers and contractors to comply with certified AI audit standards, further incentivizing industry participation.

By embedding these elements into the market ecosystem, the governance model ensures that AI systems are subject to continuous scrutiny and improvement, fostering trust among all stakeholders—developers, deployers, regulators, and the public—while encouraging innovation under a framework of accountability and transparency. *This process is inherently long-term, requiring incremental progress over several years and likely maturing over decades. However, this should not deter us from taking the necessary first steps to initiate the development of this ecosystem.*

Congress, especially the Senate, has demonstrated an interest in exploring the intersection of standards and how to enforce compliance. Here are a few examples of bills that have been introduced in the Senate during the last couple of years in this area:

- The “TEST AI Act of 2024”, **US Congress: S. 3162, 118th Cong. (2024)** mandates the creation of AI testbeds for trustworthy system development, involving interagency collaboration, risk assessments, and classified facilities to prevent AI misuse. It emphasizes red- and blue-teaming methodologies for vulnerability evaluations and aims to strengthen national security and critical infrastructure protection.
- The “AI Research, Innovation, and Accountability Act of 2023”, **US Congress: S. 3312, 118th Cong. (2023)** promotes AI innovation while ensuring accountability through transparency, risk management frameworks, and generative AI system disclosures. It mandates transparency reports for high-impact AI systems, recommends best practices for government AI adoption, and encourages robust AI oversight to mitigate risks in sensitive sectors.
- The “VET AI Act”, **US Congress: S. 4769, 118th Cong. (2024)** directs NIST to develop voluntary guidelines for AI assurance, focusing on internal and external evaluations of AI systems. It aims to enhance trust through meaningful assurances, safeguard privacy,

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

mitigate harms, and support adopting trustworthy AI solutions via evidence-based standards and technical validation.

- The “Future of Artificial Intelligence Innovation Act of 2024”, **US Congress: S. 4178, 118th Cong. (2024)**, establishes and codifies an AI Safety Institute, promotes innovation via testbeds and capacity-building initiatives, and supports international AI standards and research collaborations.

Each bill involves NIST in developing AI standards, metrics, and methodologies to ensure safety and accountability and emphasize collaboration between public and private sectors, academia, and international partners for AI research and development.

On a side note, the concept of regulatory markets introduced in the last decade in academic and AI research lab circles presents an innovative approach to governance by addressing the weaknesses of traditional government-led regulation and industry self-regulation. (Clark & Hadfield, 2019) This model focuses on governments setting clear regulatory goals while private regulators compete to deliver effective solutions that meet these objectives. By fostering competition, the approach drives innovation in regulatory technologies, enabling oversight mechanisms to keep up with the rapid evolution of AI systems. Regulatory markets tackle this issue by delegating responsibilities to private entities, incentivizing them to create advanced tools and methodologies for auditing, monitoring, and safeguarding AI systems. These private regulators operate under governmental supervision to maintain accountability while allowing for a more flexible and adaptive regulatory framework. Despite its promise, the regulatory market model faces challenges, particularly in maintaining robust government oversight and preventing regulatory capture. Nevertheless, it offers a dynamic pathway to align AI development with societal safety and ethical norms. (Carvao, 2024)

### Accountability and liability

The third and final step of the Dynamic Governance Model is the establishment of a robust system of accountability and liability. This step addresses the question of who is responsible when AI systems cause harm or fail to meet established standards and has historically proven to be the most challenging to implement. Accountability mechanisms are critical to ensuring that AI’s promises (innovation, efficiency, and better decision-making) do not come at the expense of security, safety, fairness, or human rights.

A helpful reference for understanding the importance of liability frameworks is the experience with social media platforms under Section 230 of the Communications Decency Act. Section 230’s liability shield enabled the rapid growth of the Internet and Web 2.0 by protecting platforms from being held liable for user-generated content. While this provision facilitated unprecedented innovation and economic growth, it also attracted criticism for allowing platforms

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

to evade responsibility for harmful content. This example illustrates the delicate balance between encouraging innovation and ensuring accountability—a balance that must now be carefully navigated in the context of AI. (Carvao, 2023)

Liability in the AI ecosystem introduces new complexities due to the distributed nature of AI development and deployment. Unlike traditional product liability, where responsibility can often be traced to a single manufacturer, AI systems are developed and deployed through a multi-layered supply chain. Key actors include **developers** (the entities that create and train AI models), **deployers** (those who integrate and implement AI models into products or services), and **end users** (Individuals or organizations that operate AI-driven systems in specific contexts). The NTIA Accountability Report emphasizes the need to ensure accountability across this entire value chain, highlighting that liability should not rest solely on one actor but be shared proportionally based on each actor's level of control and responsibility. For example, developers may be held accountable for transparency and design flaws, while deployers could be responsible for ensuring that AI systems are used appropriately and safely. The NTIA report identifies several areas where changes in law and policy are required to support AI accountability:

1. **Privacy:** Stronger protections are necessary to prevent AI systems from infringing on individuals' privacy. These include clear rules on data usage, retention, and sharing and requirements for transparent disclosures about AI system behavior.
2. **Copyright:** With AI models increasingly trained on vast datasets, including copyrighted materials, new legal frameworks are needed to clarify AI developers' and content creators' rights and obligations.
3. **Safety:** AI systems that pose risks to physical safety—such as autonomous vehicles and medical devices—should be subject to sector-specific safety regulations, including mandatory pre-deployment testing and certification.

Topics such as privacy and copyright reform are among the most challenging to address and represent areas lacking a prevailing normative consensus. The model's modular, lightweight, and broadly applicable design becomes especially valuable when confronting these difficulties. *Rather than beginning with these complex issues, one can first focus on areas of more explicit agreement to build trust in the model. Once trust is established, the same approach and process can be gradually extended to more protracted issues.*

Effective enforcement of accountability and liability frameworks will require a coordinated effort across multiple institutions, each playing a distinct and complementary role. **Congress** will be instrumental in establishing the legislative foundation for AI accountability, including codifying baseline liability standards and mandating sector-specific regulations where necessary. Additionally, Congress can create mechanisms for ongoing regulatory oversight to ensure these frameworks remain effective and adaptive as AI technology evolves. Even though no AI bills

## **RFI on the Development of an AI Action Plan – The Dynamic Governance Mod**

A Notice by the National Science Foundation on 02/06/2025

have been enacted into law, there has been active work during the 118<sup>th</sup> Congress in this direction. Here are several examples: the “AI Fraud Deterrence Act”, **U.S Congress: H.R. 10125, 118th Cong. (2024)** increases penalties for financial crimes such as mail, wire, and bank fraud committed using AI. The “Artificial Intelligence Civil Rights Act of 2024”, **US Congress: S. 5152, 118th Cong. (2024)** establishes protections against discrimination by computational algorithms in key areas like employment, housing, and healthcare and outlines transparency, individual rights, and enforcement mechanisms to safeguard civil rights against algorithmic bias and harmful outcomes. The “NO FAKES Act of 2024”, **US Congress: H.R. 9551, 118th Cong. (2024)** protects intellectual property rights related to individuals’ voice and visual likeness, addressing unauthorized digital replicas created using AI. It includes provisions for civil action against violations and safe harbor rules for online services that promptly remove infringing content upon notification. Each bill includes provisions for enforcement, penalties, or legal recourse to ensure compliance.

**Sectoral regulatory agencies**, such as the FDA for healthcare and the SEC for financial markets, will oversee the implementation of AI-specific regulations within their respective domains. These agencies will be tasked with certifying high-risk AI systems before deployment and ensuring compliance with established safety and ethical standards. They will play a crucial role in maintaining public trust in AI systems used in critical sectors by providing targeted oversight.

**Courts** will also serve as a vital component of the enforcement ecosystem. As disputes arise, courts interpret liability standards and resolve conflicts, setting legal precedents shaping how accountability is distributed across the AI supply chain. Over time, judicial rulings will help clarify ambiguous areas in legislation and regulation, contributing to developing a more robust and well-defined framework for AI governance.

Existing legal frameworks can also address challenges associated with AI. For example, the recent legal advisories issued by California Attorney General Rob Bonta highlight how state laws—including consumer protection, civil rights, competition, and data privacy laws—can be applied to AI systems. These advisories emphasize that AI does not exist in a legal vacuum and that businesses and developers are subject to longstanding legal principles. For instance, under California’s Unfair Competition Law, practices like deceptive advertising of AI capabilities or the misuse of AI for fraudulent purposes are actionable. Similarly, civil rights laws protect against bias and discrimination perpetuated by AI systems, while privacy laws ensure that AI developers handle sensitive data responsibly. These measures underscore the potential to adapt existing legal standards to novel technologies like AI, providing a pathway for governance that leverages familiar structures while addressing emerging risks. Such an approach enables policymakers to bridge the gap between innovation and accountability without necessitating

## RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

entirely new regulatory frameworks for every technological advance. (State of California Department of Justice, 2025)

While not an exact comparison, other domains draw on established frameworks in fields like product safety certification, financial accounting, and insurance regulation, where robust systems of accountability and liability have been successfully developed and implemented over the years. We discussed product safety certification examples such as UL. We also touched upon Financial Accounting and systems like U.S. GAAP and IFRS, offering lessons in transparency and compliance enforced by regulatory bodies such as the SEC. In insurance regulation in fields like healthcare and automotive industries, companies are often required to carry liability insurance to cover potential damages caused by their products or services. This model can be adapted to AI, where high-risk systems might similarly require mandatory insurance or contributions to compensation funds to safeguard against unforeseen harms.

By building on these established approaches, the AI ecosystem can adopt proven mechanisms—such as codified liability rules, independent oversight, and incentivization of best practices—to foster a culture of responsibility and trust. These lessons inform the following steps that can help operationalize a system of accountability and liability:

1. **Codification of Liability Standards:** Congress should pass legislation establishing clear liability standards for AI systems, including rules for determining fault across the AI supply chain.
2. **Sector-Specific Regulations:** Regulatory agencies should develop detailed, sector-specific guidelines for AI deployment. These guidelines should include pre-deployment testing, certification, and post-deployment monitoring requirements.
3. **Insurance and Compensation Funds:** Companies deploying high-risk AI systems could be required to carry liability insurance or contribute to compensation funds designed to cover potential damages.
4. **Auditor and Certifier Accreditation:** Independent auditors and certifiers should be accredited by recognized bodies to ensure consistent and reliable evaluations of AI systems. These auditors be key in identifying potential risks and ensuring compliance.
5. **Incentivizing Best Practices:** Policymakers could create incentives for companies that adopt best practices in AI accountability, such as tax benefits or reduced regulatory burdens for certified systems. These incentives will encourage proactive compliance.

*While building a comprehensive framework for AI accountability and liability is a long-term process, early steps such as establishing baseline liability standards and launching sector-specific pilot programs can set the foundation for a mature and effective system. Over time, this framework can evolve to reflect new technological developments, emerging risks, and lessons learned from real-world deployments.*

## **RFI on the Development of an AI Action Plan – The Dynamic Governance Mod**

A Notice by the National Science Foundation on 02/06/2025

Ultimately, ensuring accountability and liability in AI will require significant legal and regulatory advancements. Much of this must be codified into laws and statutes, clearly defining liability across the AI supply chain. Courts will play a crucial role in interpreting and applying these laws, setting precedents that refine liability standards over time. *While this is a complex and long-term process, establishing a solid legislative and judicial foundation is essential for fostering trust, promoting innovation, and safeguarding societal well-being in an AI-driven future.*

### **Implementation context**

The proposed Dynamic Governance Model aligns well with the U.S. approach to policy implementation, integrating elements of antitrust, sectoral regulation, and litigation. It employs antitrust principles to facilitate ex-post corrections when market concentration or anti-competitive behavior undermines the public interest. Implementing sectoral regulations provides ex-ante safeguards, establishing clear rules and standards before any harm occurs. Furthermore, the model incorporates aspects of tort law by emphasizing liability throughout the AI supply chain, where courts will play a vital role in interpreting these standards and establishing legal precedents.

This hybrid approach reflects the U.S.'s ability to balance innovation with regulation, ensuring that technological progress is not stifled but guided responsibly. *By adopting this model, the U.S. can enhance its geopolitical standing in AI leadership, outpacing global competitors such as China by demonstrating that democratic governance can foster innovation and accountability. Unlike top-down regulatory regimes, this model emphasizes transparency, fairness, and stakeholder involvement, which can strengthen trust in U.S.-led AI initiatives on the international stage.*

Codifying liability standards, creating audit ecosystems, and fostering public-private partnerships will enable the U.S. to maintain its AI geopolitical, technical, and economic leadership. Furthermore, by collaborating with international partners on harmonized standards, the U.S. can build global coalitions for responsible AI governance, ensuring interoperability, enhancing trust, and promoting shared ethical values. Most importantly, this model promotes trust—both domestically and internationally—by demonstrating a commitment to ethical AI development, ensuring safety and fairness while fostering continued innovation.

# RFI on the Development of an AI Action Plan – The Dynamic Governance Mod

A Notice by the National Science Foundation on 02/06/2025

## References

- Atkinson, R. D. (2022). *How the IT Sector Powers the US Economy*. <https://itif.org/publications/2022/09/19/how-the-it-sector-powers-the-us-economy/>
- Carvao, P. (2023, May 11). *Resetting the Rules for Tech to Preserve the Public Interest* | TechPolicy.Press. Tech Policy Press. <https://techpolicy.press/resetting-the-rules-for-tech-to-preserve-the-public-interest>
- Carvao, P. (2024). The dual imperative: Innovation and regulation in the AI era. *International Journal of Technology Policy and Law*, 3(3), 236–251. <https://doi.org/10.1504/IJTPL.2024.142861>
- Clark, J., & Hadfield, G. K. (2019). Regulatory Markets for AI Safety. *arXiv (Cornell University)*. <https://doi.org/10.48550/arxiv.2001.00078>
- Kagan, J. (2023, January 30). *Underwriters Laboratories (UL): Meaning, Overview, History*. Investopedia. <https://www.investopedia.com/terms/u/underwriters-laboratories-ul.asp>
- Nihill, C. (2024, December 20). Bipartisan Senate bill would establish an AI safety office in Commerce. *FedScoop*. <https://fedscoop.com/bipartisan-senate-bill-ai-safety-office-commerce/>
- NTIA. (2024, March 27). *AI Accountability Policy Report* | National Telecommunications and Information Administration. <https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report>
- State of California Department of Justice. (2025, January 13). *Attorney General Bonta Issues Legal Advisories on the Application of California Law to AI*. State of California - Department of Justice - Office of the Attorney General. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-issues-legal-advisories-application-california-law-ai>
- The White House. (1995, November 8). *Technology and Economic Growth*. <https://clintonwhitehouse5.archives.gov/textonly/WH/EOP/OSTP/html/techgrow.html#intro>
- The White House. (2023, July 21). *FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI*. The White House. <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>