

Chapter	Key Findings	Key recommendations
Government Use	<ul style="list-style-type: none"> • Not all AI systems need the same level of oversight. Simple tools should have fewer restrictions than powerful AI systems handling sensitive data. • AI should help people make decisions, not replace them. Rules should make sure humans stay involved when needed. • If AI is used in government decisions that affect people, those people should be informed and have a way to challenge the decision. 	<ul style="list-style-type: none"> • Ensure AI rules fit within current federal laws on data, security, privacy, and procurement to prevent conflicts and inefficiencies. • AI policies must evolve with technology, giving agencies the authority to implement changing standards effectively. • Agencies must notify individuals when AI significantly influences government decisions and provide clear processes for appeals and human review. • Clearly define AI roles, establish career pathways, and prioritize hiring based on skills rather than traditional degrees.
Federal Preemption of State Law	<ul style="list-style-type: none"> • AI regulation should not be one-size-fits-all—the way an AI system is used should determine the rules that apply to it. • There should be a flexible approach to preemption, Congress can set federal floors (minimum standards) or ceilings (maximum limits) on state AI laws, allowing some state-level regulation while maintaining federal oversight. • Any federal preemption law must clearly define AI to avoid overregulating simple tools or failing to cover high-risk systems. 	<ul style="list-style-type: none"> • Congress should study how federal and state laws impact AI in different industries to better understand regulatory gaps and overlaps. • Policymakers should examine how federal preemption would affect AI governance, ensuring it balances national consistency with state-level flexibility.
Data Privacy	<ul style="list-style-type: none"> • Large datasets improve AI performance but risk exposing sensitive information. • Many Americans have limited control over how their personal data is collected, used, and shared. • No comprehensive U.S. federal privacy law leads to confusion, with varied state regulations. 	<ul style="list-style-type: none"> • The government should support ways to share data safely, like creating privacy-protected public datasets, using synthetic data (fake but realistic data), and developing secure technologies that allow data analysis without exposing personal details. • Instead of adding privacy protections after AI is built, developers should design AI systems that collect only necessary data, protect user information, and give people control over their data. Congress can support partnerships to make these privacy-first AI systems the standard. • Privacy laws should be broad enough to cover all types of technology, not just AI, so they stay relevant as technology changes.
National Security	<ul style="list-style-type: none"> • U.S. adversaries are rapidly developing AI for military use. To stay ahead, the U.S. must invest in cutting-edge AI for defense. • AI can help the Department of Defense save time and money by automating tasks like financial 	<ul style="list-style-type: none"> • Strengthen Oversight through briefings and hearings with experts from both inside and outside the government • Promote AI Training within the military and integrate AI into existing processes.

	<p>management, auditing, and other administrative work.</p> <ul style="list-style-type: none"> AI systems in the military must work even in difficult environments where communication is limited or disrupted. The U.S. should develop secure, independent AI systems for these situations. 	<ul style="list-style-type: none"> Maintain Human Control over critical systems to uphold ethical and safety standards. The U.S. should work with allies to establish global norms and agreements for responsible AI use in military operations to enhance global security.
<p>Research, Development and Standards</p>	<ul style="list-style-type: none"> Government support for AI research through agencies like NSF, NIH, DOD, and DOE has been crucial for progress. Developing cutting-edge AI requires powerful computers and massive amounts of data. The U.S. should ensure researchers have access to these critical resources. AI has benefited from open collaboration, but some companies are keeping their research secret for competitive reasons. The government should encourage knowledge-sharing while protecting innovation. 	<ul style="list-style-type: none"> The U.S. should deepen collaboration with like-minded countries on AI research, governance, and standardization to counter authoritarian AI practices and promote democratic values. Congress should support initiatives like the U.S. Science Envoy Program and federal R&D programs that facilitate joint research projects, shared AI infrastructure, and international AI talent exchange.
<p>Civil Rights and Civil Liberties</p>	<ul style="list-style-type: none"> Flawed or biased AI can lead to discrimination, legal violations, and harm to constitutional rights Evaluating AI models for biases and limitations is essential to ensuring fair decision-making and protecting civil rights. 	<ul style="list-style-type: none"> Require Human Oversight in High-Stakes AI Decisions Develop AI Standards to Improve Accountability Federal agencies must safeguard against discriminatory AI use both within government and in sectors like banking, healthcare, housing, education, and law enforcement. Sectoral regulators should explore when and how individuals should be informed when AI is used in important decisions, particularly in law enforcement, elections, and public services.
<p>Education and Workforce</p>	<ul style="list-style-type: none"> There should be new training programs to upskill the workforce for AI-integrated jobs. The U.S. lags behind other nations in K–12 math and science, making stronger STEM education critical for developing future AI talent. Skilled workers without traditional degrees can contribute to AI development through certificate and industry training programs. K–12 educators require resources and professional development to effectively teach AI literacy in schools. 	<ul style="list-style-type: none"> The U.S. needs better data on AI jobs—what skills are needed, where job gaps exist, and how the AI workforce is changing—to create better education and training programs. AI workforce training should be designed to fit local industry needs, whether it’s manufacturing, healthcare, or tech. AI careers shouldn’t just be for people with college degrees. Skills-based hiring and alternative training, like certificate programs, should open up AI jobs to more people.

		<ul style="list-style-type: none"> • AI could replace some jobs, so existing job training and retraining programs should be reviewed and updated to help affected workers transition to new careers. • AI is changing the workplace, and the government should monitor whether current labor laws protect workers' rights in AI-driven jobs.
<p>Intellectual Property</p>	<ul style="list-style-type: none"> • Many AI-related IP issues are currently being decided in court, so Congress should be cautious about passing new laws too soon. • Many artists and content creators are unaware if their copyrighted material was included in AI training datasets • If U.S. laws overly restrict AI development, companies may move operations to countries with more AI-friendly copyright policies, while stronger protections for creators may drive talent elsewhere. 	<ul style="list-style-type: none"> • Congress should clearly define whether AI-generated content can be copyrighted or patented and how human creators' rights are protected when AI is involved in the creative process. • Let Courts Resolve fair use questions before enacting broad legislation. • Congress should create legal protections that allow people to control how their image, voice, or identity is used by AI while ensuring laws do not violate free speech rights.
<p>Content Authenticity</p>	<ul style="list-style-type: none"> • Technical solutions like watermarks or digital signatures can help but are not foolproof, as they can be faked or removed. • Teaching people to recognize AI-generated content is helpful, but even informed individuals can still be deceived by highly realistic fake content. • Secure digital identity systems, if designed with strong privacy protections, could help verify content creators and reduce the spread of fake or manipulated content online. 	<ul style="list-style-type: none"> • Policymakers should assess current copyright, privacy, and fraud laws to determine whether they effectively address AI-generated content risks. • AI-generated content has legitimate uses, so policies should target proven harms—such as fraud or misinformation—without restricting free speech or legitimate content creation. • Congress should explore legal requirements for AI developers, content creators, and platforms to disclose when content is AI-generated and improve transparency. • Congress should examine whether individuals harmed by AI-generated content, such as deepfake forgeries or fraud, have adequate legal protections and ways to seek redress.

<p>Open and Closed Systems</p>	<ul style="list-style-type: none"> • Current research suggests that open AI models do not pose enough risk to warrant restrictions, though future advancements may require reassessment. • Open-source AI fosters breakthroughs, accelerates research, and supports competition, benefiting industries and government agencies, including the Department of Defense. 	<ul style="list-style-type: none"> • AI policies should focus on clear, demonstrated harms rather than imposing unnecessary restrictions on developers without evidence of risk. • Congress should evaluate how AI could be misused in high-risk areas such as Chemical, Biological, Radiological, and Nuclear (CBRN) Threats • While current evidence does not justify restricting open-source AI, Congress should establish monitoring mechanisms to detect emerging risks and respond appropriately.
<p>Energy Usage and Data Centers</p>	<ul style="list-style-type: none"> • The rapid expansion of AI technologies is increasing electricity consumption, which may lead to supply shortages, higher energy costs, and grid reliability challenges. • Innovations in AI hardware, data center design, and energy management can help reduce power consumption • While data centers can be built quickly, expanding power generation and transmission infrastructure takes years, that's why it requires planning to meet AI's future energy needs. 	<ul style="list-style-type: none"> • Data center operators should voluntarily report energy usage and forecasts to federal agencies like the Energy Information Administration to enhance power demand planning and prevent grid strain. • Creating a common framework for measuring and benchmarking AI data center energy use would improve transparency and allow for better comparisons of efficiency across different technologies. • The costs of expanding energy infrastructure to support AI growth should be primarily covered by the tech industry, not shifted onto residential or small business ratepayers.
<p>Small Business</p>	<ul style="list-style-type: none"> • High costs for AI infrastructure, such as computational power and data, make it difficult for small businesses to compete with larger firms. • Small businesses may struggle to comply with AI-related regulations, as they lack the legal and financial resources that large companies have to manage compliance. 	<ul style="list-style-type: none"> • Support small businesses by providing access to computational power, AI-ready datasets, and capital through partnerships with agencies like the Small Business Administration and NIST. • Conduct research to identify financial and resource barriers that small businesses face when adopting AI, including industry-specific challenges. • Ensure AI regulations consider the disproportionate impact on small businesses, with clear, sector-specific rules and accessible technical assistance for compliance.
<p>Agriculture</p>	<ul style="list-style-type: none"> • Only 27% of U.S. farms use AI tools, hampered by high costs and rural connectivity gaps. • AI-powered precision agriculture can optimize input use, improve soil and water health, reduce costs, and increase crop yields. • Many farms lack reliable internet, which hinders their ability to use AI-powered precision agriculture and other advanced farming technologies. 	<ul style="list-style-type: none"> • The USDA should assess its current programs to identify ways to help farmers afford and integrate AI technologies for precision agriculture • Federal agencies should fund and deploy AI technologies to improve forest monitoring, predict wildfire risks, and assist land managers in conservation efforts. • Congress should continue reviewing the CFTC's regulatory framework to ensure it effectively addresses AI-driven risks in financial markets.

Healthcare

- AI speeds drug development, improves diagnostics, and optimizes resources but faces data bias and interoperability issues.
- Siloed data and inconsistent reimbursement policies slow broader AI adoption.

- Policymakers should foster collaboration among AI developers, healthcare providers, and regulators to establish voluntary standards for data sharing, patient privacy, and AI oversight.
- Continued investment in AI-related research, particularly through NIH, is crucial for advancing AI applications in healthcare
- As AI becomes more involved in diagnosis and treatment decisions, policymakers should establish legal frameworks to determine responsibility when AI tools produce harmful errors.
- Adapt Medicare and Insurance Reimbursement for AI-Powered Care

Financial Services

- AI models must be trained on high-quality, representative data to prevent bias, errors, and compliance issues with anti-discrimination laws.
- AI-powered tools can help underserved and underbanked communities gain access to essential financial services.
- AI is actively deployed for fraud detection, underwriting, investment research, customer service, and cybersecurity monitoring.
- Larger institutions have more resources to invest in AI, while smaller financial firms struggle to keep up

- Regulators should allow financial firms to use AI to lower costs and improve services while ensuring they follow existing laws.
- Agencies should use AI themselves to better understand how it works and how to oversee its use in the financial sector
- Congress should ensure AI in banking, loans, and housing is fair and does not lead to discrimination or harm customers.
- Regulators should create “sandboxes,” or safe test environments, to experiment with AI in financial services before making rules.