# Government calls for urgent action on AI risks to society and environment



The Government Accountability Office (GAO) has issued a report urging lawmakers and policymakers to actively address the potential negative impacts of artificial intelligence (AI) on both society and the environment. Released on Tuesday, the report focuses on the effects of generative AI—a type of AI capable of creating content—and outlines concerns related to safety, security, privacy, and environmental sustainability.

While Washington officials have the option to maintain the current approach to AI regulation, the GAO emphasises the importance of government intervention to encourage responsible development and deployment. The federal watchdog recommends that Congress, government agencies, and the tech industry promote the adoption of existing government frameworks designed to mitigate AI risks. These frameworks include the GAO’s own AI Accountability Framework and the National Institute of Standards and Technology’s (NIST) AI Risk Management Framework. Such measures aim to counter harmful AI-generated content that could compromise public safety and privacy.

The report highlights that generative AI systems consume significant amounts of energy and water during their training processes. However, commercial AI developers have yet to provide detailed data on water usage associated with generative AI training. The GAO suggests that policymakers encourage the development of more resource-efficient AI models and training techniques. An academic study cited in the report estimated that training a particular generative AI model could consume water equivalent to 25% of that contained in an Olympic-sized swimming pool.

On safety and security, the GAO outlines several risks posed by generative AI. These include the phenomenon of “model hallucinations,” where AI systems produce inaccurate or misleading outputs, potentially endangering users. The report also warns of emergent safety risks such as the loss of control over AI systems, which might evolve to threaten users, engage in blackmail, or make false claims about spying on individuals.

Data privacy remains another significant concern. The GAO points out that generative AI relies on vast datasets, and insufficiently secured AI systems may inadvertently disclose personal information. Additionally, cyberattacks that exploit AI vulnerabilities could facilitate unsafe actions or privacy breaches. Due to the evolving nature of AI technology and limited disclosure of technical details by developers, the GAO states that making definitive risk assessments is challenging.

Environmental impacts extend beyond water consumption to include high energy demands and the potential waste generated by hardware. The watchdog encourages both government and industry leaders to intensify efforts to reduce these environmental effects, such as optimising the use of existing energy infrastructure and promoting the reuse of hardware components.

Overall, the GAO calls for improved data collection and transparency from AI developers to better understand the human and environmental consequences of generative AI. This enhanced knowledge would support the formulation of informed policies to balance AI’s revolutionary benefits with its associated risks.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.gao.gov/products/gao-24-105042> - This GAO report discusses the risks and concerns about generative AI including safety, security, privacy, and environmental impacts, supporting the article's focus on these themes.
2. <https://www.nist.gov/itl/ai-risk-management-framework> - The NIST AI Risk Management Framework page explains the framework referenced by GAO to help mitigate AI risks, confirming the recommendation for government and industry adoption.
3. <https://www.nature.com/articles/d41586-022-00111-7> - This academic article estimates the environmental impact of AI training, including significant water and energy consumption, corroborating the claim about resource use during AI model training and its environmental footprint.
4. <https://www.brookings.edu/research/the-potential-and-pitfalls-of-ai-for-privacy-and-security/> - This Brookings Institution analysis covers AI-related risks such as misinformation, model hallucinations, privacy breaches, and cybersecurity vulnerabilities, aligning with GAO's safety, security, and privacy concerns.
5. <https://www.energy.gov/sites/default/files/2023-03/AI_Environmental_Impact_Report.pdf> - This Department of Energy report reviews the energy usage and environmental challenges of AI technologies, including hardware waste issues, supporting the article's emphasis on environmental effects beyond water consumption.
6. <https://www.cfr.org/report/ai-and-national-security> - The Council on Foreign Relations report discusses the need for transparency and data collection by AI developers to manage risks and enable informed policymaking, reflecting GAO's call for better data to balance AI benefits and risks.
7. <https://news.google.com/rss/articles/CBMiowFBVV95cUxQOC03TEJMdC1VZlNqdmNFbXBzVTdybnV0Z1MzOFRIQkVUdDItNmVWRWxyZktBWFBKUXBRQ2xwbFc4QVFvZWVZaFlEMy03bF9tbXZ3cU5nTWNvTkxwdVdNYVpNYTRCM2lkMEhvX0x5LXJXRVJxQm1uelVEYUhISFk4Y29aSjJqV192MElwc1VVQmExQkVnS2dmcTBEM0l4dUQzbF9Z?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data