MEMORANDUM

To: Members and Staff, Energy and Commerce Committee

From: Majority Committee Staff

Re: Energy and Commerce Full Committee Hearing on Artificial Intelligence

---

On Wednesday, December 13, at 10:00 a.m. (ET), the Committee on Energy and Commerce will hold a full committee hearing in 2123 Rayburn House Office Building. The hearing title is "Leveraging Agency Expertise to Foster American AI Leadership and Innovation."

I. WITNESSES

The following witnesses have been invited to testify:

- **Helena Fu, Director of the Office of Critical and Emerging Technology, Office of the Undersecretary for Science, Department of Energy**
- **Saif Khan, Senior Advisor for Critical and Emerging Technologies, Department of Commerce**
- **Dr. Micky Tripathi, the National Coordinator for Health Information Technology, Health and Human Services**

II. OVERVIEW

According to the Congressional Research Service (CRS), Artificial Intelligence (AI) "can broadly be thought of as computerized systems that work and react in ways commonly thought to require intelligence, such as the ability to learn, solve problems, and achieve goals under uncertain and varying conditions."[1] Researchers and federal agencies have been working on forms of AI since the 1940s and 1950s, but there have been major advancements in the field over the last decade. This is in part due to increased funding for research and development, the availability of big data to train AI models, and advances in hardware such as AI chips and high-performance computing.[2]

AI is being used to solve complex problems in diverse fields such as the health care, energy, and telecommunications sectors. While there are many opportunities and benefits to

---

[1] Laurie A. Harris, *Artificial Intelligence: Background, Selected Issues, and Policy Considerations*, R46795, Congressional Research Service, May 19, 2021, https://crsreports.congress.gov/product/pdf/R/R46795.
[2] *Id.*

deploying AI technologies, there are also inherent risks associated with AI use. These risks include data privacy considerations, a lack of transparency, the potential for bias or misuse, and cybersecurity concerns. Understanding these benefits and risks can help policy makers better ensure that AI is built and used ethically and in a way that minimizes risks to society.

Earlier this year, tech companies such as Microsoft, Meta, OpenAI, and Alphabet released chatbots, powered by AI, for public use. These chatbots, a form of generative AI technologies, use billions of data points and advanced probabilistic algorithms to mimic human writing and communication styles as it answers users' questions, writes code, and generally carries on conversations as if it were human.[3] While generative AI technology represents just one facet of this topic, it also provides Congress with an opportunity to examine broader AI issues.

This fall, the Committee held a series of hearings across the subcommittees to explore the role of AI in different sectors of the economy.[4] This full committee hearing will discuss how to balance the risks associated with AI generally and the need to keep the U.S. at the forefront of innovation, so that the U.S. can compete with our foreign adversaries like China, and implement policies that reflect our democratic values.[5]

III. BACKGROUND

Artificial Intelligence and Government

Given the rapid advancement and deployment of AI technologies, government agencies must keep pace with industry to support innovation and mitigate risks. The Departments of Commerce (Commerce), Energy (DOE), Health and Human Services (HHS), will all play important roles as AI technologies are utilized in their respective sectors of the economy.

On October 30, 2023, the Biden administration released a sweeping Executive Order (EO) on the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which outlines key administration policies and principles for overseeing and deploying AI as well as the responsibilities and duties of various executive agencies.[6] The EO directs more than

---

[3] Busch, Kristen, *Generative Artificial Intelligence and Data Privacy: A Primer*, R47569, Congressional Research Services, 1-3, May 23, 2023, https://crsreports.congress.gov/product/pdf/R/R47569.
[4] Press Release, Chairs Rodgers and Bilirakis Kick Off AI Hearing Series with Subcommittee Hearing on Safeguarding Americans' Data, Washington, D.C. (Oct. 11, 2023), https://energycommerce.house.gov/posts/chairs-rodgers-and-bilirakis-kickoff-ai-hearing-series-with-subcommittee-hearing-on-safeguarding-americans-data.
[5] *Economic Danger Zone: How America Competes to Win the Future Versus China: Hearing Before the Subcomm. on Innovation, Data, and Commerce of the H. Comm. on Energy and Commerce*, 118th Cong. (2023); https://energycommerce.house.gov/events/innovation-data-and-commerce-hearing-is-entitled-economic-danger-zone-how-america-competes-to-win-the-future-versus-china.
[6] Exec. Order No. 14110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Federal Register 75191, Nov. 1, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

50 federal entities to engage in more than 100 specific actions to implement guidance in a variety of policy areas including:[7]

- Safety and security
- Innovation and competition
- Worker support
- Consideration of AI bias and civil rights
- Consumer protection
- Data Privacy
- Federal use of AI
- International leadership

In addition to the EO, agencies must also consider how to implement other government-wide guidance on the use, regulation, and monitoring of AI technologies. For example, the Office of Management and Budget (OMB) released a draft memorandum proposing guidance for the agency use of AI, which outlines specific steps agencies should take, including designating Chief AI Officers, convening AI governance boards, and developing strategies for advancing agency use of AI, and publicly releasing AI use case inventories.[8] Further, the Government Accountability Office's (GAO's) AI Accountability Framework identifies key practices to help ensure accountability and responsible use by federal agencies and other entities involved in the design, development, deployment, and continuous monitoring of AI systems.[9]

AI and Innovation, Data, and Commerce

AI and Data Privacy

The debate around AI has highlighted that the U.S. does not have a comprehensive federal data privacy and security law to guard against the misuse of personal information, while other countries around the world have put in place such a foundation. In the U.S., the lack of a uniform national framework has led to a patchwork of rules and regulations that can cause confusion for consumers, gaps in privacy protections, compliance burdens and uncertainty for businesses, while at the same time hampering AI developers, innovators, and creators.[10]

---

[7] Laurie A. Harris & Chris Jaikaran, *Highlights of the 2023 Executive Order on Artificial Intelligence for Congress*, R47843, Congressional Research Service, 1, Nov. 17, 2023, https://crsreports.congress.gov/product/pdf/R/R47843
[8] Proposed Memorandum for the Heads of Executive Departments and Agencies: Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence, Office of Management and Budget 1, 26, Nov. 1, 2023, https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf
[9] GOV'T ACCOUNTABILITY OFFICE, GAO-21-519SP, ARTIFICIAL INTELLIGENCE: AN ACCOUNTABILITY FRAMEWORK FOR FEDERAL AGENCIES AND OTHER ENTITIES (2021), https://www.gao.gov/assets/gao-21-519sp.pdf.
[10] Andrew Folks, *US State Privacy Legislation Tracker* (September 15, 2023), International Association of Privacy Professionals. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

Data used to train AI models is collected in a variety of ways. Some companies use a combination of internal and external data.[11] Other firms, such as those deploying large scale models, mostly rely on data harvested from the internet. Data harvesting is a process by which data, often publicly available information, is copied from the internet. There have been many cases where an individuals' personal information or legally protected intellectual property have been copied into training data sets.[12] Some companies package this data and sell it to firms while others create open-source data sets for developers, like LAION (Large-scale AI Open Network).[13] This large-scale data collection has spurred conversations regarding data ownership, with some tech companies establishing systems to minimize and deter scraping, arguing that scraping diminishes user experience.[14] In contrast, others argue that such freely available information on the internet should be "fair game."[15]

U.S. Federal AI Frameworks

In collaboration with the private and public sectors, the National Institute of Standards and Technology (NIST) has developed a framework to manage better the risks to individuals, organizations, and society associated with AI. The NIST AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.[16]

AI in the Energy Sector

Office of Science and Research Infrastructure

While the DOE was founded in 1977,[17] its Advanced Scientific Computing Research (ASCR) program in its Office of Science has been exploring AI issues since the 1960s.[18] The

---

[11] Sara Brown, *Why External Data Should Be Part of Your Data Strategy*, MIT SLOAN SCHOOL OF MGMT., Feb. 18, 2021, https://mitsloanmit.edu/ideas-made-to-matter/why-external-data-should-be-part-your-data-strategy.
[12] Kevin Schaul, Szu Yu Chen, & Nitasha Tiku, *Inside the secret list of websites that make AI like ChatGPT sound smart*, Washington Post (Apr. 19, 2023), https://wapo.st/3S071CL.
[13] Marissa Newman & Aggi Cantrill, *The Future of AI Relies on a High School Teacher's Free Database*, Bloomberg (Apr. 23, 2023), https://www.bloomberg.com/news/features/2023-04-24/a-high-school-teacher-s-free-image-database-powers-ai-unicorns#xj4y7vzkg.
[14] Reuters, *Twitter now requires users to sign in to view tweets* (June 30, 2023), https://www.reuters.com/technology/twitter-now-needs-users-sign-view-tweets-2023-06-30/.
[15] Marissa Newman and Aggi Cantrill, *The Future of AI Relies on a High School Teacher's Free Database*, Bloomberg (Apr. 23, 2023), https://www.bloomberg.com/news/features/2023-04-24/a-high-school-teacher-s-free-image-database-powers-ai-unicorns#xj4y7vzkg.
[16] Nat'l Inst. Of Standards and Tech., *AI Risk Management Framework*, https://www.nist.gov/itl/ai-risk-management-framework.
[17] DEP'T OF ENERGY, OFFICE OF LEGACY MGMT., *Brief History of the Department of Energy*, https://www.energy.gov/lm/brief-history-department-energy#:~:text=Activated%20on%20October%201%2C%201977,of%20nuclear%20weapons%20dating%20from (last visited Nov. 21, 2023).
[18] DEP'T OF ENERGY, OFFICE OF SCI., *DOE Explains…Artificial Intelligence*, https://www.energy.gov/science/doe-explainsartificial-intelligence (last visited Nov. 21, 2023).

ASCR program has contributed to the development of hardware and software necessary for the next generation of AI technologies.[19] The DOE's cutting-edge supercomputers, algorithms, and large scientific datasets are valuable assets for further AI development.[20] The DOE stated it is working with U.S. firms to progress computing and AI capabilities at scale.[21]

Energy Sector Applications

AI has multiple applications in the energy sector. These uses include predicting potential electric equipment malfunctions, identifying damaged electric infrastructure in the wake of storms, optimizing oil and gas operations, and evaluating the risk of wildfires.[22] For example, AI can address the complex computational challenges of optimizing power flow for the electric grid.[23] AI-guided drones can also capture images of damaged electric equipment.[24] The DOE's Office of Cybersecurity, Energy Security, and Emergency Response supports the application of AI in the energy sector, such as by funding activities across its National Laboratories and communicating with industry partners. National Laboratories researchers have explored the use of AI to improve grid operations. For example, researchers at Argonne National Laboratory (ANL) have developed AI capabilities to assist grid operators in long-term forecasting, facilitating their consideration of more scenarios and better expansion planning.[25] Researchers at ANL are also merging grid expertise with this lab's advanced computing facilities to develop new methods of extracting information from large amounts of grid data to improve grid reliability and efficiency.[26] Additionally, researchers at the DOE's Pacific Northwest National Laboratory (PNNL) are exploring the use of AI techniques to predict, plan for, and respond to disasters such as wildfires.[27]

Energy Sector Risks

---

[19] *Id.*
[20] DEP'T OF ENERGY, *Innovation, Safety, and Security*, Oct. 31, 2021, https://www.energy.gov/articles/innovation-safety-and-security-doe-leads-ai.
[21] *Full Committee Hearing to Examine Recent Advances in Artificial Intelligence and the Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging Technologies: Hearing Before the S. Comm. on Energy and Natural Res.*, 118th Cong. (2023) (statement of David Turk, Deputy Secretary, Department of Energy).
[22] *The Role of Artificial Intelligence in Powering America's Energy Future: Hearing Before the Subcomm. on Energy, Climate, and Grid Security of the H. Comm. on Energy and Commerce*, 118th Cong. (2023) (statement of Edward Abbo, President and Chief Technology Officer, C3 AI); *id.* (statement of Paul Dabbar, Distinguished Visiting Fellow, Center on Global Energy Policy, Columbia University).
[23] *Id.* (statement of Jeremy Renshaw, Senior Technical Executive - AI, Quantum, and Innovation, Electric Power Research Institute).
[24] *Id.* (statement of Paul Dabbar, Distinguished Visiting Fellow, Center on Global Energy Policy, Columbia University.)
[25] Christina Nunez, *Artificial Intelligence Can Make the U.S. Electric Grid Smarter*, ARGONNE NAT'L LAB., June 19, 2019, https://www.anl.gov/article/artificial-intelligence-can-make-the-us-electric-grid-smarter.
[26] *Id.*
[27] Steven Ashby, *PNNL Researchers Using AI to Aid Disaster Response and Recovery*, PAC. NORTHWEST NAT'L LAB., Sept. 25, 2023, https://www.pnnl.gov/news-media/pnnl-researchers-using-ai-aid-disaster-response-and-recovery.

Despite the potential benefits, the proliferation of AI also poses unique and evolving threats to the energy sector, including its infrastructure. These include cybersecurity risks and data security challenges.[28] For example, while AI can potentially secure energy infrastructure from cyberattacks,[29] bad actors could also employ AI to launch their attacks.[30] Additionally, hardware and software produced in adversarial nations such as China could also contain "physical back doors" or gaps in algorithms to facilitate sabotage.[31]

AI in Communications Technology

Networks

AI applications are being used throughout communications networks. In recent years, network operators have used AI to manage traffic, optimize network performance, and even predict potential problems before users could be affected.[32] AI is used to monitor and automate core network functions, which some network operators have found to reduce the number of outages.[33] Additionally, AI enables communications providers to improve customer service.[34] Some providers use AI to improve the speed and quality of responses to consumer inquiries about their broadband subscriptions.[35]

AI applications also power advancements in wireless networks and the devices to which they connect. For example, 5G and future generations of wireless networks rely on advanced computing power at the edge of the network to enable better quality of service and more efficient uses of spectrum.[36] Specifically, both the networks and devices can learn and improve upon the way they use spectrum within the unique environment where they are operating. AI applications are being used to improve how signals are transmitted off of, around, or through obstacles, known as beamforming.[37] Additionally, advanced wireless networks use AI to improve their security by detecting patterns that suggest malicious activity.[38] Implementing AI solutions into

---

[28] *The Role of Artificial Intelligence in Powering America's Energy Future: Hearing Before the Subcomm. on Energy, Climate, and Grid Security of the H. Comm. on Energy and Commerce*, 118th Cong. (2023) (statement of Jeremy Renshaw, Senior Technical Executive- AI, Quantum, and Innovation, Electric Power Research Institute)
[29] *Id.* (statement of Edward Abbo, President and Chief Technology Officer, C3 AI).
[30] *Id.* (statement of Jeremy Renshaw, Senior Technical Executive- AI, Quantum, and Innovation, Electric Power Research Institute).
[31] *Id.* (statement of Paul Dabbar, Distinguished Visiting Fellow, Center on Global Energy Policy, Columbia University).
[32] Dean Takahashi, *Comcast Credits AI Software for Handling the Pandemic Internet Traffic Crush*, VentureBeat (July 13, 2020), https://venturebeat.com/business/comcast-credits-ai-software-for-handling-the-pandemic-internet-traffic-crush/; Jeff Heynen, *AI's Impact on Broadband Networks,* Dell'Oro Group (Aug. 10, 2023), https://www.delloro.com/ais-impact-on-broadband-networks/.
[33] Heyen, *supra* note 7.
[34] Rose de Fremery, *How AI Customer Service Can Help Enable Better Interactions*, Verizon (accessed Oct. 25, 2023), https://www.verizon.com/business/resources/articles/s/how-ai-customer-service-can-help-enable-better-interactions/.
[35] *Id.*
[36] Dr. Tingfang Ji, What's the Role of Artificial Intelligence in the Future of 5G and Beyond?, Qualcomm (Sep. 20, 2021), https://www.qualcomm.com/news/onq/2021/09/whats-role-artificial-intelligence-future-5g-and-beyond.
[37] *Id.*
[38] *Id.*

the Radio Access Network (RAN) and network core may also improve the performance of wireless broadband networks by predicting and managing changes in traffic.[39] As network operators continue to define and design the networks of the future, AI applications are expected to continue to adapt.

Communications networks also leverage AI applications to prevent the scourge of robocalls. When implementing the TRACED Act, the Federal Communications Commission (FCC) permitted carriers to block certain calls, many of which utilize analytics and automated technologies.[40] While these are not a comprehensive accounting of the uses of artificial intelligence by network operators, they highlight the diversity of uses that exist. On the other hand, AI can also pose challenges, such as mimicking human voices for mass robocalls.[41] On October 23, FCC Chairwoman Jessica Rosenworcel announced plans to circulate a Notice of Inquiry exploring how AI affects illegal robocalls, including protecting consumers from such calls under the Telephone Consumer Protection Act (TCPA).[42]

Cybersecurity

AI has revolutionized the approach to spotting cyber threats and possibly malicious activities by providing advanced techniques to detect and mitigate cyber threats. AI systems are using machine learning algorithms that can detect malware, run pattern recognition, and detect even the smallest behaviors of malware or ransomware attacks before it enters the system.[43]

AI's ability to "learn" from previous behavior allows for rapid, actionable insights when confronted with new or unfamiliar information or behaviors. It can make logical inferences based on potentially inadequate data subsets and provide several solutions to a known problem, allowing security teams to choose the best course of action. New, generative AI can recreate human speech and writing, allowing hackers to create complex phishing attacks that were traditionally beyond their reach.[44] With the ability to identify deep fakes, malicious actors have a better capability to trick financial institutions and family members into exposing sensitive information based on their belief that the caller's identity is trusted.[45] The most prominent

---

[39] *From Reactive to Proactive Network Operations*, Ericsson (accessed Oct. 25, 2023), https://www.ericsson.com/en/ai/operations.
[40] "In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls," Declaratory Ruling and Third Further Notice of Proposed Rulemaking, Federal Communications Commission (CG Docket No. 17-59). Rel. June 7, 2019. Available at: https://docs.fcc.gov/public/attachments/FCC-19-51A1.pdf.
[41] *See, e.g.*, Sam Sabin, *Generative AI Is Making Voice Scams Easier To Believe*, Axios Codebook (Jun 13, 2023), https://www.axios.com/2023/06/13/generative-ai-voice-scams-easier-identity-fraud.
[42] *FCC Chairwoman Launches Effort to Better Understand AI's Impact on Robocalls and Robotexts,* Federal Communications Commission (Oct. 23, 2023), https://docs.fcc.gov/public/attachments/DOC-397925A1.pdf.
[43] Gaurav Belani, *The Use of Artificial Intelligence in Cybersecurity: A Review*, IEEE: Computer Society (accessed Oct. 25, 2023), https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity.
[44] Sam Sabin, *ChatGPT-Written Phishing Emails Are Already Scary Good*, AXIOS (Oct.24, 2023), https://www.axios.com/2023/10/24/chatgpt-written-phishing-emails.
[45] Roman H. Kepczyk, *Deepfakes Emerge as Real Cybersecurity Threat*, AICPA & CIMA (Sep. 28, 2022), https://www.aicpa-cima.com/news/article/deepfakes-emerge-as-real-cybersecurity-threat.

response to these new AI hacking capabilities is AI empowered cybersecurity.[46] Security systems that incorporate AI capabilities have impressive capabilities in the detection of malicious activities, malware detection, and proactive threat hunting.[47] The complexity of AI-empowered cyberattacks highlights the need for sector-specific cybersecurity, so that those with understanding of the subject matter can identify deep fakes and fraud.

AI in Healthcare

Drug Development

Drug development is currently a high-risk endeavor where a small number of commercially successful drugs compensate for a much larger number of unsuccessful developments. Some 90 percent of potential treatments that enter Phase I trials fail.[48] As one academic paper noted, "[n]o other major business type operates under such a high failure rate".[49] Moreover, drug development is also a very time-consuming and costly process. It takes on average ten years and up to $10 billion to develop a new drug.[50]

AI has the potential to expedite and de-risk the drug development process. Initial uses include target identification in the preliminary stages of development where, "AI is being trained on large datasets, including omics datasets, phenotypic and expression data, disease associations, patents, publications, clinical trials, research grants, and more to understand the biological mechanisms of diseases and to identify novel proteins and/or genes that can be targeted to counteract those diseases."[51] AI can also assist drug developers by predicting drug properties thereby theoretically reducing the need for costly testing of drug candidates.[52]

Because of its potential, the deployment of AI in drug development is expected to grow rapidly. By one estimate, revenue related to AI assisted drug development is expected to reach $4.8 billion by 2028 as compared to $0.9 in 2023.[53] HHS, especially the Food and Drug Administration (FDA), will need to adapt to the increasing role of AI in drug development to

---

[46] Gaurav Belani, *AI for Cybersecurity and Cybercrime: How Artificial Intelligence is Battling Itself*, IEEE: Computer Society (Sep. 6, 2023), https://www.computer.org/publications/tech-news/trends/ai-fighting-ai; https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/.
[47] *Id.*
[48] Derek Lowe, *The Latest on Drug Failure and Approval Rates*, Science (May 9, 2019), https://www.science.org/content/blog-post/latest-drug-failure-and-approval-rates.
[49] *Id.*
[50] Cong. Budget Office, Research and Development in the Pharmaceutical Industry (2021), https://www.cbo.gov/system/files/2021-04/57025-Rx-RnD.pdf.
[51] Matthew Chun, *How Artificial Intelligence is Revolutionizing Drug Discovery*, BILL OF HEALTH, PETRIE-FLOM CTR. AT HARVARD LAW SCHOOL, Mar. 20, 2023, https://blog.petrieflom.law.harvard.edu/2023/03/20/how-artificial-intelligence-is-revolutionizing-drug-discovery/#:~:text=According%20to%20Morgan%20Stanley%2C%20even,more%20than%20%2450%20billion%20opportunity.
[52] *Id.*
[53] Shawn Zeller et al., *AI, Drug Development, and Big, Big, Bucks*, POLITICO, Nov. 20, 2023, https://www.politico.com/newsletters/future-pulse/2023/11/20/ai-drug-development-and-big-big-bucks-00127961.

ensure the safety and efficacy of AI developed drugs while not unnecessarily delaying ability of companies to bring life-saving AI developed treatments to market.

Improving Diagnosis & Patient Care

AI and machine learning technologies are already available to assist doctors and other medical professionals with diagnosing disease and patient care. Diagnostic errors are one of the most common and costly medical errors. By one estimate, these errors negatively impact more than 12 million Americans and result in unnecessary medical costs of more than $100 billion.[54] While adoption of AI to assist with patient diagnosis is in its infancy, it shows great potential to reduce rates of misdiagnosis and to improve patient care by synthesizing and making available to medical providers vast amounts of clinical data.[55]

For example, AI technologies that interpret radiology image data sets are already being deployed to analyze images and identify similarities, which can help medical providers diagnose patients.[56] However, despite the advantages provided by AI technologies, surveys have shown that clinicians and patients remain reluctant to use it, particularly for technologies that do not allow a health care professional to use their independent professional judgment.[57] This suggests that, for the foreseeable future, AI will remain primarily a tool to assist medical professionals in improving the accuracy of diagnosis and patient care.

Fraud Detection

Health care fraud is estimated to cost the United States up to $300 billion annually and represents an estimated 3 to 10 percent of total healthcare spending. With respect to Medicare, the HHS Office of Inspector General (OIG) has found that fraudulent billing and prescription writing schemes often follow certain patterns.[58] A medical provider suspected of fraudulently billing Medicare for services that were never performed may standout for performing an unusually large numbers of a certain procedure when compared to his or her peers.[59] The same applies for prescribing patterns. This suspicious billing pattern can inform HHS OIG and the Department of Justice investigations.

Traditionally, the volume of Medicare claims submitted for payment has prevented law enforcement from systematically identifying suspicious billing or prescribing patterns. Because

---

[54] U.S. GOV'T ACCOUNTABILITY OFFICE, *Machine Learning's Potential to Improve Medical Diagnosis*, WATCHBLOG, Nov. 10, 2023, https://www.gao.gov/blog/machine-learnings-potential-improve-medical-diagnosis.
[55] *Id.*
[56] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-22-104629, ARTIFICIAL INTELLIGENCE IN HEALTH CARE: BENEFITS AND CHALLENGES OF MACHINE LEARNING TECHNOLOGIES FOR MEDICAL DIAGNOSTICS 25 (2009), https://www.gao.gov/products/gao-22-104629 .
[57] Chiara Longoni & Carey K, Morowedge, *AI Can Outperform Doctors. So Why Don't Patients Trust It?*, HARV. BUS. REV., Oct. 30, 2019, https://hbr.org/2019/10/ai-can-outperform-doctors-so-why-dont-patients-trust-it.
[58] *See* DEP'T OF JUSTICE AND DEP'T OF HEALTH AND HUMAN SERVS., ANNUAL REPORT OF THE DEPARTMENTS OF HEALTH AND HUMAN SERVICES AND JUSTICE, HEALTH CARE FRAUD AND ABUSE CONTROL PROGRAM FY 2022 (2023), https://oig.hhs.gov/publications/docs/hcfac/FY2022-hcfac.pdf
[59] *Id.*

of its ability to analyze large data sets for patterns, AI has the potential to assist payors and investigators in identifying suspicious patterns indicating potential fraud.[60] In January of this year, HHS announced that it would launch a pilot program to "streamline fraud identification" by the Centers of Medicare and Medicaid Services (CMS).[61] The National Institutes of Health (NIH) have also launched a similar AI pilot program to analyze grant proposals.[62] Balanced against AI's potential to identify patterns associated with fraud, waste, or abuse, is the very real risk that AI's pattern based approach will sweep too broadly and bring under investigation innocent health care providers.[63]

Dual Use Research and Biosecurity Considerations

With advances in AI capability and expanding accessibility, experts are increasingly concerned that AI, and generative AI in particular, has the potential to proliferate knowledge regarding the manufacturing of dangerous pathogens and biological weapons.[64] An exercise by MIT students illustrates AI's dual use potential:

> MIT students recently demonstrated how large language model (LLM) chatbots could be used to help non-experts understand the process of manufacturing risky pathogens. Within one hour, students without science backgrounds had used the chatbots to list four viruses capable of causing a pandemic, identify reverse genetics as a means to manufacture them and suggest acquisition methods that could help bypass misuse screening.[65]

In short, the same capacity that allows AI to analyze large data sets to predict promising potential drugs and treatments development can be used for nefarious purposes. The Center for Arms Control and Non-Proliferation has concluded that "machine learning has progressed far enough that current AI capabilities are able to allow bad actors to flip the switch and go from being a helpful tool of medicine to being a generator of weapons."[66]

---

[60] Jayla Whitfield, *How Health Tech Leaders Use AI to Combat Fraud*, GovCIO, Mon. 22, 2023, https://governmentciomedia.com/how-health-tech-leaders-use-ai-combat-fraud.
[61] Nihal Krishan, *HHS CIO Mathias Says Tree-Based AI Models Helping to Combat Medicare Fraud*, FedScoop, Jan 18, 2023, https://fedscoop.com/hhs-cio-mathias-says-tree-based-ai-models-helping-to-combat-medicare-fraud/#:~:text=AI-,HHS%20CIO%20Mathias%20says%20tree%2Dbased%20AI%20models%20helping%20to,according%20to%20the%20IT%20leader.&text=U.S.%20Department%20of%20Health%20and%20Human%20Service%20Chief%20Information%20Officer%20Karl%20Mathias.
[62] *Id.*
[63] Dan Martin, *Federal Agencies Using Generative AI, Analytics to Search for Health Care Fraud*, Med. Econ., Sept. 12, 2023, https://www.medicaleconomics.com/view/federal-agencies-using-generative-ai-analytics-to-search-for-health-care-fraud.
[64] Janet Egan & Eric Rosenback, *Biosecurity in the Age of AI: What's the Risk*, Belfer Ctr., Harvard Kenndy School, Nov. 6, 2023, https://www.belfercenter.org/publication/biosecurity-age-ai-whats-risk.
[65] *Id.*
[66] Sophy Macartney, *Biological Threats Have Evolved for the Worse, and We Are Not Prepared*, Ctr. For Arms Control and Non-Proliferation, Sept. 1, 2023, https://armscontrolcenter.org/biological-threats-have-evolved-for-the-worse-and-we-are-not-prepared/.

IV. KEY QUESTIONS

The hearing may include discussion around the following key questions:

1. What AI technologies are being developed, deployed, and used in different sectors of the economy?
2. What are some of the benefits and risks of these technologies?
3. What are the policy implications and data privacy considerations for these technologies and how can lawmakers balance innovation and economic growth with consumer protection and other risks?
4. How do U.S. investments, use, and governance of AI development and deployment compare to other countries?
5. How are government agencies preparing to research, deploy, and regulate AI technologies?
6. How are government agencies coordinating and collaborating with private industry and outside groups when developing or regulating AI?

V. STAFF CONTACTS

For questions regarding the hearing, please contact Sean Brebbia or Deep Buddharaju of the Committee staff.