Testimony of Helena Fu

Director, Office of Critical and Emerging Technologies

U.S. Department of Energy

Before the

House Committee on Energy & Commerce

December 13, 2023

Chair Rodgers, Ranking Member Pallone, and distinguished Members of the Committee, thank you for the opportunity to testify on behalf of the Department of Energy's (DOE's) vision for and activities in Artificial Intelligence (AI). All of us in DOE particularly appreciate the interest, leadership, and partnership from this Committee at this critical juncture in AI development.

Advances in AI are enabling enormous progress and breakthroughs that can help address key challenges of our time – from more effective cancer screening and targeted treatments to world-changing advanced manufacturing, from improving the reliability of our electricity grid and response to natural disasters, to state-of-the-art production capabilities for our nuclear stockpile. At the same time, the rapid pace of AI development, accelerating investment by global competitors, and widespread AI access also carry unprecedented risks.

This testimony will first outline the Department of Energy's substantial AI foundation and experiences to date. It will secondly outline the full range of broader AI trends and dynamics with respect to our core energy, science, and national security missions. Finally, the testimony will discuss DOE's role in implementing the Administration's recent Executive Order on Safe, Secure, and Trustworthy AI and present for the Committee's consideration a vision for how DOE can play our role to best harness AI breakthroughs and to mitigate AI's unprecedented risks.

DOE's AI foundation

Let me begin by thanking this Committee for your strong support of DOE for many years that has helped enable DOE's existing infrastructure and capabilities for cutting-edge AI. These extensive capabilities to date include:

- Advanced computing: DOE designed, developed, and currently operates four of the top ten fastest openly-benchmarked supercomputers in the world – DOE's Frontier supercomputer, the Nation's first exascale supercomputer, is currently the fastest – and Congress's investments have been critical to ensuring continued U.S. leadership in the supercomputing industry. DOE labs are also involved in driving emerging green and AI-optimized computing innovations in collaboration with industry.
- Advanced software: DOE has created a wealth of science and engineering algorithms that can run on the most advanced supercomputers, as well as on emerging green & AI-

optimized advanced computing solutions. Through efforts like the Exascale Computing Project, DOE is developing the world's first capable exascale software ecosystem that will drive breakthroughs in critical areas as varied as extreme weather and climate risks, materials science, AI, cancer research, earthquake risk assessment and prevention, energy production and storage, supply chain optimization, grid planning and resiliency, and nuclear security applications.

- Largest producer of unclassified and classified scientific data: Across a network of 34 national user facilities around the country, DOE provides the scientific community with instruments to enable research while also generating tremendous volumes of high-quality data. DOE also maintains data and digital products that are vital to the development and validation of advanced AI solutions for energy and societal needs.
- Largest skilled scientific workforce: Most importantly, DOE's National Laboratory system houses a workforce of over 70,000 scientists, engineers, researchers, and support personnel with world-leading scientific expertise, and serves as a resilient talent and training pipeline for personnel who serve the American people.

It is particularly important to underscore that DOE advances in AI are not just in the realm of the future. On average, DOE-supported research contributes one new AI method or evaluation technique applicable to multiple scientific domains every single day. DOE is currently leveraging in real-time our core strengths in AI applications and leading high-performance computing systems to deliver across our energy, security, and science mission:

Energy:

- Driving energy efficiency in computing: As more and bigger AI models are trained and deployed, more chips are expected to consume significant amounts of electricity. DOE has a long history of innovating at the leading edge in energy efficient computing at multiple scales. Our national labs have achieved in a 200-fold reduction in energy per floating point operations per second (a measure of computer performance) over two decades. In addition to being the world's fastest publicly benchmarked supercomputer, Frontier is also ranked #2 in the world on energy efficiency.

- Accelerating clean energy deployment and energy accessibility: DOE and its labs have worked with States, local governments, Tribes, cities, and communities across the country and around the world to help implement clean energy solutions. AI is being used to conduct the complex analytics, forecasting, and technology road mapping necessary to help plan energy investments that could potentially shorten the timeframe for planning and permitting critical infrastructure from years to weeks. Researchers at our national labs are using AI to rapidly model new energy transition pathways, develop unique solutions that take into account a community's existing infrastructure, and improve decision making for new infrastructure, resulting in improved energy resilience, greater peak load flexibility or reduced carbon footprint.

- Enhancing efficiency and safety: With nearly a million wells across the country producing roughly 13 million barrels of crude oil and 6.7 million barrels of natural gas liquids per day, the United States now stands as the world's largest producer of these

resources. AI has the potential to increase output, efficiency, and worker safety. In fact, DOE is already utilizing AI to help determine the condition of undocumented orphan wells and evaluate the integrity and potential for reuse of conventional energy infrastructure for carbon capture and storage, making these assets safer and evaluate opportunities for potential alternative uses for commercial and societal benefit. We are also using AI to increase efficiency in industrial processes. DOE partnerships with industry have applied AI techniques and our supercomputing resources to improve the energy efficiency of a manufacturing process for melt-blown nonwoven material used in N95 masks.

- Protecting our electric grid: Infrastructure modernization has the potential to advance the effectiveness of energy system operations, but can also come with increased security risks. Rapid adoption of smart sensing devices is generating a surge of data that promises greater visibility into the health of the power grid – and AI and data analytics can help turn that data into actionable intelligence for grid operators and utilities. However, as these tools expand in capability, so does the potential that malicious actors might seek to target them directly – or to use other forms of AI and machine learning to enhance their attempts to attack our critical energy systems. This is why our national labs have partnered with industry, academia, and a national service organization to develop secure artificial intelligence/machine learning tools to detect and mitigate cyber-attacks on electric power distribution systems and microgrids. This includes the development of algorithms that can detect and mitigate attacks, establishment of a hardware-in-the-loop testbed and demonstration test plan development, and construction of a red team software test environment. As we look to support the operators of our evolving energy system, we are looking at how deep analysis of cascading electrical system failure data can help evaluate the effectiveness of remedial action schemes, identify critical restoration elements, and compare the cost of different plans to ensure a more reliable and resilient system.

- Improving clean energy generation: Advanced AI/ML methods are already supporting the DOE's Energy Earthshot Initiative to accelerate research, development, and demonstration breakthroughs in more abundant, affordable, and reliable next-generation clean energy technologies and solutions by 2035. An Energy Earthshot Research Center focused on floating offshore wind aims to make floating offshore wind a long-term viable energy source, and will develop new understanding of key phenomena associated with meteorological and oceanic conditions and use scientific machine learning to swiftly advance the design and control of floating offshore wind turbines and farms and their integration with the grid. Similarly, DOE's AI-enabled science-based models have identified new domestic sources of clean energy resources, and unconventional critical minerals. This breakthrough will simultaneously reduce our reliance on critical mineral imports while supporting clean energy community transitions. Many of these unconventional critical mineral resources coincide with conventional fossil energy systems, offering a pathway for jobs and communities to benefit.

Nuclear Security and Nonproliferation:

- Nuclear nonproliferation and nuclear security: DOE laboratories are pursuing research in foundation models for nuclear nonproliferation and nuclear security applications in HPC, cloud, and hybrid environments, making inroads in testing and evaluation, and addressing transparency, usability, and robustness in human-AI teaming. DOE national lab researchers partnered with academia to demonstrate the first real-time digital twin of a nuclear reactor. Digital twinning, combined with machine learning technologies, can lead to new innovations in process-monitoring detection, such as data tampering. It represents a technological leap in evaluation and detection capability to safeguard any nuclear facility.

- New materials discovery: DOE is using AI methods, including machine learning, to enhance and extend pit production, additive manufacturing of new components, component/system surveillance, design of new experiments, and proliferation detection. National Nuclear Security Administration (NNSA) laboratories have active AI development programs for materials discovery, which have shortened the time for analytical processes for critical weapons materials from weeks to seconds and uncovered key interactions among new materials.

- Understanding future threats: NNSA is also utilizing computing and algorithmic innovations to improve dynamic decision support - from partnering with DOD to better understand the battlefield of the future to discovering and countering novel proliferation pathways. DOE will also partner with the interagency to assess the potential role for AI in enhancing defenses against new cyber threat vectors and enhance the security of systems (whether physical or virtual) from all threats and hazards.

- Nuclear Threat Reduction and Information Security: NNSA laboratories are assessing the various ways in which AI and machine learning could enhance an adversary's understanding of nuclear threat devices. NNSA is working with industry to analyze AI model outputs and inform potential future development of mitigations that can be implemented to prevent AI from aiding malevolent actors.

- Secure data management and integration: NNSA has a multi-laboratory program to develop a federated data management system for all nuclear nonproliferation and nuclear security research data, which would ultimately operate across multiple classification data fabrics, enable colocation of data with compute resources, both high performance computing and cloud services, and integrate with other government data management systems to enable transformative research in nuclear nonproliferation and nuclear security.

Science and Technology:

- Transformative advances in computing hardware for AI: Large-scale AI training commonly relies on large deployments of computing hardware, such as graphics-processing units (GPUs). Critical components of that computing hardware were initially developed thanks to DOE's exascale computing investments, which helped these components achieve aggressive targets for energy efficiency, performance, and

reliability. DOE is working with leading U.S. firms to advance computing and AI capabilities at scale.

- Breakthrough in Fusion: DOE-sponsored basic research in magnetic-confinement fusion demonstrated innovative AI techniques to predict plasma instabilities. The recent groundbreaking net-positive-energy fusion demonstration from the National Ignition Facility at Lawrence Livermore National Laboratory was enabled by DOE's development and application of these novel AI methods.

- Understanding the evolution of the virus behind COVID-19: Our national laboratories have partnered with academic institutions and hardware companies to develop a prize-winning AI based on "large language model" techniques – using the language of the virus genome instead of the language of humans – to understand the evolution of the virus behind COVID-19. Our labs have also leveraged broad expertise in AI, biology, and chemistry, together with computing resources, to accelerate development of medical countermeasures for vaccines, enhancing pandemic preparedness and bioassurance capabilities.

- Accelerating time to discovery: National lab researchers have developed AI tools to enable a form of "speed reading" in microscopy, possibly revolutionizing data collection and allowing scientists to preserve precious samples, such as easily degradable biological materials or miniscule quantities of novel quantum materials, and reduce time using expensive X-ray, electron, and atomic probe microscopes. This technique uses AI to selectively target points of interest for scanning and identifying clusters of important features and speeding time to discovery.

- Assisting in emergency response: DOE researchers have used AI-based image analytics and models to assess damage and predict risks, providing situational awareness and damage assessments within hours of a natural disaster or other emergency, to assist the Coast Guard with modeling fire spread and evacuation efforts in Maui.

- DOE also develops and maintains authoritative data and digital products that are vital to the development and validation of advanced AI solutions for energy and societal needs. Data are the "energy" for AI and are vital for testing, validation and building trust, especially for complex energy-related analyses.

Promising opportunities

AI is a powerful technology that presents breathtaking opportunities for our nation, and the Biden-Harris Administration has taken historic actions, including through its October 30th Executive Order, to maximize these benefits and maintain the United States' technological advantage while ensuring that AI upholds our democratic values, advances equity and delivers inclusive prosperity.

We are working under the leadership of the White House and in close partnership with interagency colleagues to leverage complementary capabilities. For example, in support of the

Executive Order on AI and the National AI Research Resource, DOE announced an extension of the Summit supercomputer at Oak Ridge National Laboratory through October 2024. This extension will enable researchers to pursue AI projects on one of the world's leading AI-enabled open science supercomputing platforms. In addition, users of DOE's Frontier and Summit supercomputers can take advantage of a unique infrastructure that provides resources and protocols that enable researchers to safely and securely process protected data at scale, including personally identifiable information, data protected under export-controlled information regulations, and other types of data that require privacy.

Over the next decade, AI can help unlock world-leading simulation capabilities that can be augmented seamlessly with scalable, trusted, and efficient data-driven tools, including trusted and validated machine learning methods, and greater use of complementary AI technologies and beyond. DOE will need to harness the transformative power of AI to aid in advancing our science, energy, and security mission.

Clear-eyed about the risks

The Biden-Harris Administration is also addressing the significant risks that AI presents to our safety and security, democracy, economy, and civil and human rights. The Administration is tackling these risks head-on by securing voluntary commitments from major AI companies, issuing a landmark Executive Order on Artificial Intelligence, and releasing for public comment a draft Office of Management and Budget (OMB) policy for the use of AI by the U.S. government.

Global investment and competition in AI are increasing, and our continued leadership – whether public sector or private – is not assured. Our competitors have made significant strides in closing the capability gap to develop extremely complex systems over the last decades. For example, China has moved to replicate the model and investments of the DOE's National Laboratory system and is investing heavily in its own AI capabilities and workforce. Moreover, the introduction of powerful language models in public-facing Internet services have revealed a pressing need for fundamental understanding of new, emergent capabilities of these models and the associated risks to society.

Three factors are shifting how we need to think about AI as a country:

1. Governments around the world are investing in AI capabilities as national assets critical to future economic vitality and national security. We must move faster or risk falling behind.
2. Retaining leadership in AI will require developing trustworthy AI systems that can be deployed for high-consequence uses, from healthcare to aerospace.
3. Protecting Americans' rights and safety will require alignment of national investments and policies to evaluate and mitigate risks that can be exacerbated by AI advancements. We must protect against both unintended behaviors and AI used by those with malicious intent.

In short, a robust partnership between the government, our private sector, and like-minded allies and partners is essential to ensuring that this technology is underpinned by democratic principles and values, and that all Americans benefit from its adoption and are safe from potential harms. Given the rapid pace of AI developments, we must move quickly.

DOE's AI foundation and expertise across energy, science, and national security give us unique insight into critical AI opportunities as well as a wide spectrum of associated risks that threaten to undermine the promise of AI technologies. AI systems can pose risks to individual safety, privacy, and civil liberties; and risks to society from information manipulation, bias and discrimination, social engineering, and market manipulation; and security risks from autonomous, biological, chemical, and nuclear, radiological, and cyber weapons. DOE is already leading the way in developing trustworthy AI systems in areas such as:

- Explaining and assessing outputs: Trust is frequently a barrier to AI/ML adoption, and making AI explainable to the general public could facilitate trust by revealing how results were produced, and how certain those results are. DOE needs these capabilities in uncertainty quantification and explainability for our national security mission. Our national laboratories are developing explainability tools that enable counterfactual analysis – providing a similar, but AI-generated, sample and explaining how that would have changed outcomes – to increase user confidence in results.

- Equity and social justice: Bias is a considerable concern with AI, but AI applications could also be used to further equity and justice efforts. Leveraging AI multi-modeling (incorporating multiple types of analysis and data), including deep learning and natural language processing, we have developed a Capture & Storage Environmental Justice and Social Justice data collection and interactive map to help stakeholders and decision makers gain a more comprehensive understanding of the complex interplay between environmental and social factors that affect carbon capture and storage infrastructure projects and the communities they are located within and rely upon for support.

- Protecting information privacy and the privacy of an individual's information: Using AI can involve access to sensitive patient data that must be protected. DOE's PALISADE-X project is using federated learning to improve research outcomes by training AI on biomedical datasets from multiple health organizations while preserving patient privacy. AI models are sent to where the data is stored; health organizations can keep their own data private by not having to send it anywhere, but the model output improves because it is trained on more datasets.

While U.S. industry has had an outsized role in the development of AI technologies to the present day, industry alone cannot face this wide spectrum of risks. Given the nation-state-scale investments happening outside of our borders, our nation requires unprecedented industry-government partnership because:

- Industry alone cannot be fully aware of the relevant risks and threats because much of that information falls within the purview of our Intelligence Community and our national security enterprise.

- Industry investments are driven by market dynamics and the needs of their customers. The government, however, can help industry limit externalities that might harm individuals and society as a whole.
- Our industry-driven AI innovation ecosystem now faces nation-state competitors who have substantial resources at their disposal and a desire to overtake our leadership position.

A vision for AI leadership and DOE's role

We've discussed how the Biden-Harris Administration has been laser-focused on a comprehensive approach to AI across federal departments and agencies. In the remainder of my testimony, I will lay out our vision for DOE's vital role in implementing the Administration's AI Executive Order, with our agency peers, across the scientific community and U.S. industry, and with our allies and partners to ensure continued leadership in this new AI era. We stand ready to use our vast experience in AI and its unique capabilities, in partnership with our sister departments and agencies, to take advantage of AI opportunities while helping to understand and mitigate the risks.

This is not the first time our nation has been confronted with a technological challenge and opportunity to change society as we know it. For instance, the Manhattan Project broadly mobilized our great scientific and technical talent to meet an enormous challenge – to win the race to create the atomic bomb and end World War II. The country forged the foundations of the DOE in the Manhattan Project and as the war drew to a close, established DOE's predecessor, the Atomic Energy Commission, as a civilian agency with a dual mission: to guarantee American superiority in the new era of nuclear science for both national security and for open society, to pursue both open and classified R&D, to create a workforce with unparalleled expertise to understand and control the risks of nuclear technology in order to harness its extraordinary potential for our national security, including economic security. The results: A nuclear navy. A strong nuclear deterrent. Technology that enables our energy security. Extreme ultraviolet technology – a key component in today's microelectronics. Targeted treatments for cancer. The first map of the Human genome. Research investments in basic research from the 1960s that laid the foundations for modern day AI through sustained investments in high-performance computing, networking, data management, and algorithms.

This legacy is not just history. It is written into DOE's DNA. Our role in the Federal Government is unique – we are entrusted with one of the nation's most potent national-security assets, we contain an element of the intelligence community – and yet we are a civilian agency that is simultaneously enabling modernization of our electrical grid and the development and deployment of clean-energy technologies to strengthen our energy security and to address climate change. Our diverse and talented workforce collaborates with universities on open science questions, the private sector on proprietary R&D, and across the defense and intelligence communities to advance our national security, including energy and economic security.

Unlike the Manhattan Project, we are not starting from zero on AI, thanks again to Congressional leadership and support for many years. We already possess the enabling infrastructure –

hardware, software and talent – the fruits of billions of dollars of computing investments by the U.S. Congress over the past decade – that will enable us to move out with purpose and speed.

As governments around the world move forward on regulation of AI, the technology itself presents unique constraints. It is rapidly developing at a pace at which new capabilities can be discovered after a model is introduced to the public. Private-sector AI efforts alone will not meet the demands of the new scientific and national security competition of this AI era. The unprecedented computing ability offered by exascale computer systems represents the global stakes for AI competitiveness, but leadership will hinge on developing sustainable exascale and beyond-exascale computing environments along with the underlying theory, mathematics, and software systems necessary to utilize the power of those systems. To ensure protection of sensitive national security information while leveraging AI for our national defense, we will need to develop unique classified AI models, methodologies, and systems.

To ensure the deployment of safe, responsible, and trustworthy AI, we need to develop methods for assessing and red-teaming AI models to identify and mitigate the risks presented by cutting edge AI systems. DOE's technical expertise across multiple science and security domains, AI expertise, AI-capable hardware, and industry partnerships can be brought to bear to understand and mitigate the spectrum of AI security risks. To implement the recent AI Executive Order, DOE is working with the Department of Commerce to develop guidance and benchmarks for evaluating and auditing AI capabilities, with a focus on capabilities through which AI could cause harm, such as in the areas of cybersecurity and biosecurity. We are also conducting AI red-teaming tests to facilitate deployment of safe, secure, and trustworthy systems.

Throughout, we are working through our laboratories, with industry, and with university consortia to advance multidisciplinary research to enable technologies to train the next generation of scientists and bridge the gap between basic university research, industry requirements, and mission-specific applications.

Leveraging DOE capabilities

Effective execution of the DOE mission requires the best and most powerful scientific tools. The most promising advances in AI result from scaling, and computational capacity and capabilities are central to driving the future of AI. DOE's nationwide Exascale Computing Project (ECP) team of over 1,000 scientists, engineers, and program staff from DOE laboratories, academia, and industry, has created a vision for exascale computing and then developing, organizing, and executing a campaign to not merely lead the world but to redefine the field. In 2022, DOE's Exascale Computing Initiative (ECI) demonstrated this paradigm shift, deploying the world's first exascale supercomputer — the highest ranked world-wide, with more capability and capacity than the next four ranked systems combined. In November 2023, the second DOE exascale machine, Aurora, was brought online, and it could eventually provide twice this capacity when testing and finetuning is complete.

But advantages in AI and machine learning can only be unlocked through powerful computing capability and commensurate amounts of good data. DOE's network of scientific user facilities and sectoral responsibility for grid critical infrastructure makes us the largest generator and user

of scientific and technical data in the country. This data is a tremendous resource and asset that must be harnessed.

At DOE, we are mobilizing our National Laboratories to realize advancements in AI technology, implementation, and application. Over the last five years, we have worked with stakeholders across the innovation ecosystem to identify new and rapidly emerging opportunities and challenges presented by AI, and identified how unique DOE capabilities can drive progress in AI in our mission areas, culminating in the May 2023 release of the report AI for Science, Energy, and Security. This vision and blueprint align precisely with the pressing need for scientific grounding in areas such as bias, transparency, security, validation, and the impact of AI on jobs.

DOE is already taking action: expanding and creating research and industry partnerships to develop energy-efficient AI computing technologies, making AI resources available to the research and business communities, curating safe data sets for AI training, and using AI to accelerate the development of technologies of the future. For example, DOE national laboratories are also among the founding partners of Trillion Parameter Consortium; a global consortium of scientists from federal laboratories, research institutes, academia, and industry formed to address the challenges of building large-scale AI systems and advancing trustworthy and reliable AI for scientific discovery.

The recent Executive Order on AI charges the Department with many critical responsibilities. To advance U.S. innovation in AI, DOE will expand partnerships to utilize DOE's computing resources to build foundation models for science, energy, and national security; establish a pilot program to train 500 new scientists; contribute to the development of a Global AI research agenda and a Research Coordination Network for privacy enhancing technologies; and examine the potential for AI to improve planning, permitting, investment, and operations for the electric grid.

To mitigate AI-related risks, DOE will help conduct red-teaming tests; develop testbeds to support safe, secure and trustworthy AI; assess potential risks related to AI and critical infrastructure; evaluate the potential for AI to be misused for Chemical, Biological, Radiological, and Nuclear (CBRN) threats; minimize the risks at the convergence of AI and biology; and help identify the technical conditions for AI models and computing clusters subject to industry reporting.

Success in these efforts will require close coordination with our sister departments and agencies, as well as strong partnerships with industry and academia. At DOE, we are standing up a new office to coordinate the development of AI and other critical and emerging technologies across DOE programs and the 17 national laboratories.

Conclusion

We are now at a moment where we can – and must – focus on applications of AI which govern critical infrastructure that includes a more secure and reliable grid, enhanced emergency response, and strengthened nuclear security. In all these cases, safety, transparency, and security

are the major challenges in AI facing the scientific community and industry with many open questions.

To develop AI that we can deploy and use safely in critical environments, we need high-quality scientific data to train AI systems. We must develop AI systems that are designed to act in trustworthy ways with appropriate human oversight. Indeed, succeeding will depend on continuing to push the frontier on AI technology – and DOE has a proven history of creating and deploying technology to solve complex challenges for the United States. And, given the speed with which AI is developing and its transformative potential, we are moving with purpose to implement the recent Executive Order and leverage our existing advantages to maintain and extend U.S. leadership in AI to stay ahead of global competitors.

We are now at the cusp of our next grand challenge. Working within and outside of government, DOE stands ready to play our role in fully engaging in this grand challenge by utilizing our unique computing capacity, comprehensive and well-curated data sets from experiments and simulations, our algorithms and methods, relationships with industry, and skilled scientific workforce. We look forward to working with the Committee on this important issue.