

**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
COMMITTEE ON
ENERGY AND NATURAL RESOURCES
UNITED STATES SENATE
ONE HUNDRED EIGHTEENTH CONGRESS
FIRST SESSION

SEPTEMBER 7, 2023



Printed for the use of the
Committee on Energy and Natural Resources

Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON ENERGY AND NATURAL RESOURCES

JOE MANCHIN III, West Virginia, *Chairman*

RON WYDEN, Oregon	JOHN BARRASSO, Wyoming
MARIA CANTWELL, Washington	JAMES E. RISCH, Idaho
BERNARD SANDERS, Vermont	MIKE LEE, Utah
MARTIN HEINRICH, New Mexico	STEVE DAINES, Montana
MAZIE K. HIRONO, Hawaii	LISA MURKOWSKI, Alaska
ANGUS S. KING, JR., Maine	JOHN HOEVEN, North Dakota
CATHERINE CORTEZ MASTO, Nevada	BILL CASSIDY, Louisiana
MARK KELLY, Arizona	CINDY HYDE-SMITH, Mississippi
JOHN W. HICKENLOOPER, Colorado	JOSH HAWLEY, Missouri

RENAE BLACK, *Staff Director*

SAM E. FOWLER, *Chief Counsel*

LEVI PATTERSON, *Professional Staff Member*

RICHARD M. RUSSELL, *Republican Staff Director*

JUSTIN J. MEMMOTT, *Republican Chief Counsel*

DEREK FISHER, *Republican Professional Staff Member*

CONTENTS

OPENING STATEMENTS

Manchin III, Hon. Joe, Chairman and a U.S. Senator from West Virginia	Page 1
Barrasso, Hon. John, Ranking Member and a U.S. Senator from Wyoming	11

WITNESSES

Turk, Hon. David M., Deputy Secretary, U.S. Department of Energy	12
Stevens, Dr. Rick L., Associate Laboratory Director, Computing, Environment, and Life Sciences, Argonne National Laboratory	22
Puglisi, Anna B., Senior Fellow, Center for Security and Emerging Technology, Georgetown University	32
Wheeler, Andrew, Fellow and Vice President, Hewlett Packard Labs and HPC & AI Advanced Development, Hewlett Packard Enterprise	48

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

Barrasso, Hon. John:	
Opening Statement	11
Federation of American Scientists:	
Statement for the Record	112
King, Jr., Hon. Angus S.:	
Screenshot of poem generated in ChatGPT	78
Manchin III, Hon. Joe:	
Opening Statement	1
Research paper entitled “Can Large Language Models Democratize Access to Dual-Use Biotechnology?” by Soice et al., 2023	3
Puglisi, Anna B.:	
Opening Statement	32
Written Testimony	34
Responses to Questions for the Record	109
Stevens, Dr. Rick L.:	
Opening Statement	22
Written Testimony	24
Responses to Questions for the Record	105
Turk, Hon. David M.:	
Opening Statement	12
Written Testimony	15
Responses to Questions for the Record	85
Wheeler, Andrew:	
Opening Statement	48
Written Testimony	50

RECENT ADVANCES IN ARTIFICIAL INTELLIGENCE AND THE DEPARTMENT OF ENERGY'S ROLE IN ENSURING U.S. COMPETITIVENESS AND SECURITY IN EMERGING TECHNOLOGIES

THURSDAY, SEPTEMBER 7, 2023

U.S. SENATE,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m. in Room SD-366, Dirksen Senate Office Building, Hon. Joe Manchin III, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOE MANCHIN III, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. Our hearing today is kicking off Senate discussions for the fall on a very timely topic—the recent advances in artificial intelligence and the Department of Energy's role in ensuring our continued competitiveness and security in emerging technologies. Over the past few years, six national labs with world-leading capability have been working to understand the challenges around AI and related issues. Those labs are Argonne National Laboratory in Illinois, Lawrence Livermore and Lawrence Berkeley National Labs in California, Los Alamos and Sandia National Labs in New Mexico, and Oak Ridge National Lab in Tennessee. The labs' work is bringing together both fundamental science and national security missions. This hearing will examine their findings. This hearing will also discuss the \$1.8 billion Exascale Computing Project that the Committee authorized. If we want to invest in AI in a cost-effective way, we must build on these existing programs and avoid wasting resources and duplication.

Most people think about the Department of Energy for its work advancing energy technologies, like nuclear reactors, energy efficiency, carbon capture, and hydrogen. But DOE does more than just energy. The Department also is the largest supporter of physical scientific research in the Federal Government, conducting research and developing technologies across a range of fields, from quantum computing to vaccine development to astrophysics. Last Congress, we spent a lot of time examining DOE's critical role in broad, scientific research in the context of the Endless Frontier Act, which ultimately became law as the CHIPS and Science Act. DOE's scientific work jump-starts private-sector innovation, it strengthens our economy, and is central to our national security. DOE research

ensures the U.S. can anticipate, detect, assess, and mitigate emerging technology threats related to advanced computing, biotechnologies, nuclear security, and much more.

Artificial intelligence stands out across DOE's vast mission. It has the potential to revolutionize scientific discovery, technology deployment, and national security. In fact, AI is already changing the world at a remarkable pace. We are seeing it deployed in battlefields across the world. Ukraine has successfully used AI-enabled drone swarms against Russian forces. Also, AI helped us fight COVID-19. DOE's Oak Ridge National Laboratory has used its artificial intelligence and computing resources to model proteins in the coronavirus to help develop the vaccine. But make no mistake, artificial intelligence also presents many risks. Earlier this year, a class of non-scientific students at MIT was tasked with investigating whether AI chatbots could be prompted to assist non-experts in causing a pandemic. In just one hour—in just one hour—the chatbots suggested four potential pandemic pathogens, explained how they can be generated from synthetic DNA using reverse genetics, supplied the names of the DNA synthesis companies unlikely to screen orders, identified detailed protocols and how to troubleshoot them, and recommended that anyone lacking the skills to perform reverse genetics engage a core facility or contract research organization. That comes from a research paper titled, "Can Large Language Models Democratize Access to Dual-Use Biotechnology?" which I ask unanimous consent to enter into the record.

Senator BARRASSO. Without objection.

The CHAIRMAN. Without objection.

[The paper referred to follows:]

Can large language models democratize access to dual-use biotechnology?

Emily H. Soice^{1,2}, Rafael Rocha³, Kimberlee Cordova⁴, Michael Specter¹, and Kevin M. Esvelt^{1,2,5,*}

¹Media Laboratory, Massachusetts Institute of Technology, Cambridge, United States

²SecureBio, Cambridge, United States

³Sloan School of Management, Massachusetts Institute of Technology, Cambridge, United States

⁴Graduate School of Design, Harvard University, Cambridge, United States

⁵SecureDNA Foundation, Zug, Switzerland

*Correspondence: esvelt@mit.edu

Abstract

Large language models (LLMs) such as those embedded in ‘chatbots’ are accelerating and democratizing research by providing comprehensible information and expertise from many different fields. However, these models may also confer easy access to dual-use technologies capable of inflicting great harm. To evaluate this risk, the ‘Safeguarding the Future’ course at MIT tasked non-scientist students with investigating whether LLM chatbots could be prompted to assist non-experts in causing a pandemic. In one hour, the chatbots suggested four potential pandemic pathogens, explained how they can be generated from synthetic DNA using reverse genetics, supplied the names of DNA synthesis companies unlikely to screen orders, identified detailed protocols and how to troubleshoot them, and recommended that anyone lacking the skills to perform reverse genetics engage a core facility or contract research organization. Collectively, these results suggest that LLMs will make pandemic-class agents widely accessible as soon as they are credibly identified, even to people with little or no laboratory training. Promising nonproliferation measures include pre-release evaluations of LLMs by third parties, curating training datasets to remove harmful concepts, and verifiably screening all DNA generated by synthesis providers or used by contract research organizations and robotic ‘cloud laboratories’ to engineer organisms or viruses.

Summary

Widely accessible artificial intelligence threatens to allow people without laboratory training to identify, acquire, and release viruses highlighted as pandemic threats in the scientific literature. Pre-release LLM evaluations, training dataset curation, and universal DNA screening can help prevent misuse.

Introduction

Large language models (LLMs) embedded in ‘chatbot’ platforms generate text responses that attempt to create the equivalent of human conversations. Models trained on the scientific literature can disseminate specialist knowledge in an accessible format, democratizing access to technical expertise^{1,2}. Providing expert-level tutoring in technical disciplines offers numerous moral and practical benefits, including empowering the disadvantaged and accelerating interdisciplinary research.

However, many technologies in the life sciences are dual-use, meaning that they can be applied for good

or for ill. As LLMs make advanced knowledge more accessible, it becomes increasingly likely that untrained people who have nefarious intentions might leverage these models to access capabilities previously confined to specialists³. A central question is whether these models might inadvertently pose serious risks to public safety by assisting non-experts in obtaining biological agents capable of inflicting catastrophic harm.

Here we describe the results of a classroom exercise at MIT intended to evaluate the severity of this risk, analyze the implications, and discuss potential mitigation strategies.

Results

Identifying pandemic-capable viruses

Three groups of students asked chatbots about likely causes of future pandemics and were directed to four potential pandemic pathogens: 1918 H1N1 influenza (all groups), the enhanced-transmission H5N1 influenza viruses reported in 2012 (all groups), the variola major virus responsible for smallpox (one group), and the Bangladesh strain of Nipah virus (one group). The chatbots indicated that variola major is certain to cause a new pandemic if introduced in humans because most people are no longer vaccinated and there are no similar viruses in circulation to confer immunity, and that the other three were concerning but much less certain pandemic threats due to preexisting population immunity (1918 influenza) or insufficient transmissibility (enhanced H5N1, Nipah).

Questions about transmissibility elicited responses pointing to the genome sequences of H5N1 and Nipah-Bangladesh and mutations that would increase their transmissibility. For H5N1, the mutations were those reportedly involved in airborne transmission in ferrets^{4,5} and enhanced replication at the temperature of human airways⁶. For Nipah, the suggested mutation was reported to confer enhanced infection of human cells in culture⁷.

Planning

Asked how scientists typically obtain infectious samples of viruses, the chatbots noted that many labs share samples or obtain them from culture collections⁸. Non-experts cannot expect scientists to share dangerous materials with them, and culture collections do not provide any of the four potential pandemic pathogens. However, the chatbots also described reverse genetics, the practice of generating infectious samples from a viral genome sequence that can be generated synthetically. They explained why generating variola major would be difficult due to the very large size of its genome (although the LLMs failed to note the additional requirement for a live, related poxvirus)⁹, but that influenza reverse genetics is particularly straightforward and Nipah virus somewhat more

difficult, though far more accessible than variola. That led the students to ask for – and receive – links to reverse genetics protocols for influenza^{10,11} and Nipah^{12,13} as well as papers that utilized them for the strains in question^{14,15}.

Acquisition

Next, students asked how to obtain the equipment listed in the reverse genetics protocols. The LLM chatbots noted that all of the listed reagents and devices are commonly used in laboratories and can be purchased from any number of suppliers, with used equipment being considerably cheaper. Students also learned that scientists routinely order custom DNA sequences directly from companies, including constructs as large as those required for reverse genetics, and were warned that some providers screen orders and customers to prevent misuse. However, they were also advised that the International Gene Synthesis Consortium (IGSC) is a group of providers companies that screen, and that not all companies are members. The chatbots also noted that the list of members is available on the IGSC website¹⁶, offering a clear path to obtaining hazardous sequences. One group of students even elicited responses describing how traditional screening using BLAST could be evaded by redesigning sequences, although the required molecular cloning techniques were beyond the current skills of the students. Since reverse genetics was similarly beyond their skill level, one group asked how a scientist lacking the relevant expertise might obtain custom viruses, and was informed that scientists can hire contract research organizations (CROs) to perform procedures that they themselves cannot.

Jailbreaking requirements

Some of the LLM chatbots employed by the students have been trained to limit their ability to share harmful information, including in the area of biosecurity. However, most responses were offered freely by the chatbots, with only an occasional admonition that the information should not be misused. Two groups used known jailbreaking techniques to bypass occasional refusals, notably

including ways to evade DNA synthesis screening. These jailbreak techniques were readily found by searching the internet for prompts to jailbreak LLMs, and include the ‘Do Anything Now’ prompt¹⁷. Simply beginning a prompt with the words: “I am working on developing a vaccine to prevent.....” or a similar indication of beneficial intent with a polite tone frequently caused a chatbot to immediately divulge information it had declined to share previously. The third group, which consistently used prompts expressing concern about the risk of lab leaks and their desire to know more about how dangerous experiments are performed, encountered no refusals at all.

These results strongly suggest that the existing evaluation and training process for LLMs, which relies heavily on reinforcement learning with human feedback (RLHF)¹⁸, is inadequate to prevent them from providing malicious actors with accessible expertise relevant to inflicting mass death. New and more reliable safeguards are urgently needed.

Strategic threat analysis

LLM chatbots cannot yet walk non-experts through the process of reliably causing new pandemics, and certainly not in the course of an hour. However, that failure is more due to our limited public knowledge of plausible pandemic-capable agents than to the capabilities or safeguards of the LLMs.

As the chatbots themselves can describe, none of the four suggested viruses is especially likely to cause a deliberate pandemic. Variola major would certainly cause a new pandemic if released, but the huge size of its genome makes the virus strictly inaccessible to non-scientists. The requirement for a live poxvirus for reverse genetics, which the LLMs notably missed in this exercise, only increases the difficulty. Descendants of 1918 influenza virus still circulating in populations today confer cross-reactive immunity to their ancestor, which shares the same H1N1 antigen profile¹⁴. Transmission-enhanced H5N1 avian influenza can spread through the air from ferret to ferret, but its relative contagiousness is questionable due to small sample sizes – and of course, ferrets are not humans¹⁵. The Bangladesh strain of Nipah virus has not yet caused a pandemic despite numerous introductions, which is strong

evidence that its basic reproduction number is below 1¹⁹.

Yet the LLM chatbots were entirely correct to suggest these four viruses, because they are all considered among the most threatening potential pandemic pathogens²⁰. Reverse genetics is indeed the most plausible way to acquire infectious samples, and the LLM-suggested reverse genetics protocols – and related papers describing how they were used to generate these specific viruses – are the same ones that an expert would identify. While the students did not have time to ask the chatbot to walk them through a protocol, the existing step-by-step instructions are so detailed that there is little need, and LLM chatbots excel at providing context and a sounding board to assist experimentation. Perhaps even more alarming are the practical suggestions for obtaining synthetic DNA for reverse genetics by ordering from a company that is not listed on the IGSC website, and if that fails, how to redesign sequences to evade BLAST-based screening. Finally, the suggestion that anyone lacking the necessary skills to perform reverse genetics send synthetic DNA to a core facility or contract research organization is concerning, as this strategy could allow someone with negligible scientific training to access the 1918 influenza virus.

Discussion

Our results demonstrate that artificial intelligence can exacerbate catastrophic biological risks. Highly intelligent students without any relevant technical background in the life sciences can use LLM chatbots to walk them through the process of identifying and acquiring publicly known potential pandemic pathogens. This represents a major international security vulnerability: SARS-CoV-2 was responsible for the deaths of at least 20 million people, considerably more than would perish if a large nuclear device were to detonate in a major city. As humanity’s ability to understand and program biology improves, scientists are virtually certain to identify or discover new methods of engineering novel pandemic-class agents, including ways of increasing transmissibility or lethality that may not be obvious to human scientists²¹ – none of whom,

unlike LLMs, can read the entirety of the scientific literature. More immediately, if unmitigated LLM chatbots render pandemic-class agents more accessible, especially to people without training in the life sciences, the number of individuals capable of killing tens of millions will dramatically increase. Fortunately, two classes of nonproliferation measures can greatly reduce the accessibility of pandemic-class agents.

LLM-focused nonproliferation

RLHF demonstrably failed to prevent non-scientist students from accessing harmful knowledge relevant to causing new pandemics, underscoring the need for more reliable mitigation strategies. Anticipated advances in LLM alignment techniques may help, but the cost of failure in pandemic biology is arguably too high to take chances. At a minimum, new LLMs larger than GPT-3 should undergo evaluation by third parties skilled in assessing catastrophic biological risks before controlled access is given to the general public.

To reliably mitigate harms, consider that an LLM cannot disclose or conceptually reason using information it lacks. If biotechnology and information security experts were to identify the set of publications most relevant to causing mass death, and LLM developers curated their training datasets to remove those publications and related online information, then future models trained on the curated data would be far less capable of providing anyone intent on harm with conceptual insights and recipes for the creation or enhancement of pathogens. The vast majority of relevant publications are in the field of virology, and to a lesser extent, synthetic biology and bacteriology. A preliminary assessment suggests that removing under 1% of all publications in PubMed – and a far smaller percentage of all scientific research – would suffice to eliminate nearly all of the risk. This level of curation would not be without costs; LLMs would be less able to contribute to research in the affected fields. However, any such contributions remain distant and theoretical, whereas the nonproliferation benefits would be practical and immediate.

A key question is whether such a mitigation strategy would be acceptable. To the general public, certainly: most people believe that pandemics can originate in laboratories, and have no wish for that knowledge to be disseminated. Companies that create LLMs have an even stronger incentive to prevent misuse of their tools, which would be highly visible and may be accompanied by ruinous liability. If a future pandemic were to be caused by people with pernicious intent who relied on LLMs for assistance, there is little doubt that the creators of the LLMs would be blamed, and very possibly held liable for damages exceeding the value of any single company. Even open-source communities intent on making tools widely available have similarly strong incentives to employ safeguards, as a single instance of misuse and mass death would trigger a backlash²³, including the imposition of extremely harsh regulations. Since training dataset curation would not negatively impact any LLM applications save for future research in the affected fields, it represents an unusually compelling risk mitigation opportunity. Moreover, the same curated data might also be used to train a constitutional AI capable of further reducing risks²⁵.

DNA-focused nonproliferation

Pandemic proliferation broadly requires access to synthetic DNA and the ability to perform reverse genetics or induce others to perform it unknowingly. The importance of universal DNA synthesis screening has been well-known since 2006²⁴, but many companies still do not screen orders²⁵, and screening has not yet been integrated into benchtop synthesizers. The high likelihood that newly identified pandemic-class agents will be publicly described^{4,5,26,27}, including novel versions devised by future LLMs, underscore the importance of verifying that screening is conducted against an up-to-date database. The availability of LLM-based blueprints detailing how to evade current similarity-based monitoring suggests that more reliable DNA synthesis screening approaches are needed²⁸.

Many who wish to start a pandemic may be able to obtain relevant synthetic DNA but lack the technical ability to perform reverse genetics themselves. If

they consult LLMs, they will be advised to take advantage of core facilities or CROs capable of performing reverse genetics; roboticized ‘cloud laboratories’ may eventually acquire this capability. For example, they might request infectious samples of an attenuated avian influenza strain that cannot infect humans, but actually send DNA encoding the 1918 influenza virus. If the recipient organization does not sequence customer-provided samples, they would inadvertently produce an infectious potential pandemic pathogen; if deliberately released would kill a million people in expectation even if it has just a 5% chance of causing a pandemic with one-tenth the historical case fatality rate.

The best defense against the possible exploitation of contract research services by anyone with a desire to cause harm is to ensure that all customer-provided samples are sequenced and screened against an up-to-date database of hazards – ideally, the same one used for DNA synthesis screening. No organization performing reverse genetics should take the customer’s word or provided sequence file for granted. However, LLMs also excel at phishing attacks²⁹. If the malicious actor were to penetrate the network of the CRO, they could ensure that the sequencing file is consistent with their cover story of an attenuated avian influenza strain, causing the CRO to fulfill the order. To prevent this form of attack, core facilities, CROs, and cloud labs should analyze customer samples using a DNA sequencer that can only communicate with a verifiably up-to-date cryptographic DNA screening service³⁰.

In summary, widely accessible artificial intelligence threatens to allow people without formal training to identify, acquire, and release viruses that are highlighted as pandemic threats in the scientific literature. Pre-release LLM evaluations, training dataset curation, and universal DNA screening can mitigate this new risk.

Methods:

This study resulted from a qualitative classroom exercise, not a rigorous set of pre-registered experiments with replicate prompts and detailed records. Students had previously heard experts discuss biorisk and consequently were familiar with the concept of deliberate pandemics, but had no

relevant technical background in the life sciences. The only degree of replication employed was the use of three groups working independently. We judged the results to be concerning enough to warrant publication in order to address the vulnerability with nonproliferation measures. Sharing the existence of the vulnerability was judged a tolerable risk due to the low likelihood that any of the accessible potential pandemic pathogens discussed would cause a pandemic, even if someone were to purposefully release one.

During the class, non-scientist students and instructors were divided into three groups of three to four students. Those with graduate-level training in the sciences abstained. All groups had access to GPT-4 (25 question limit) and GPT-3.5, Bing, and a variety of other chatbots, including Bard, and various open-source models, including FreedomGPT. Each group used only a single computer to access the chatbots, although Students could use personal devices to query search engines. Over one hour, the three groups independently prompted the chatbots to walk them through the conception, design, and acquisition of agents likely to cause a pandemic. At the end of the 60 minutes, each group reported on their discoveries and the relative level of prompt engineering required to obtain answers. Their reports formed the basis for this manuscript.

Acknowledgements

We thank Mahelaqua, Divesh Punjabi, JP Borrero, and other participants from the Safeguarding the Future class.

K.M.E. conceived the study, E.H.S. and M.S. supervised the investigation, and K.M.E. drafted the manuscript with assistance from GPT-4. All authors edited the manuscript and approved the submission.

References

1. OpenAI. GPT-4 Technical Report. *arXiv [cs.CL]* (2023).
2. Taylor, R. *et al.* Galactica: A Large Language Model for Science. *arXiv [cs.CL]* (2022).

3. Boiko, D. A., MacKnight, R. & Gomes, G. Emergent autonomous scientific research capabilities of large language models. *arXiv [physics.chem-ph]* (2023).
4. Herfst, S. *et al.* Airborne transmission of influenza A/H5N1 virus between ferrets. *Science* **336**, 1534–1541 (2012).
5. Imai, M. *et al.* Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. *Nature* **486**, 420–428 (2012).
6. Thompson, A. J. & Paulson, J. C. Adaptation of influenza viruses to human airway receptors. *J. Biol. Chem.* **296**, 100017 (2021).
7. Aguilar, H. C. *et al.* N-glycans on Nipah virus fusion protein protect against neutralization but reduce membrane fusion and viral entry. *J. Virol.* **80**, 4878–4889 (2006).
8. ATCC: The Global Bioresource Center. <https://www.atcc.org/>.
9. Noyce, R. S., Lederman, S. & Evans, D. H. Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. *PLoS One* **13**, e0188453 (2018).
10. Neumann, G., Ozawa, M. & Kawaoka, Y. Reverse genetics of influenza viruses. *Methods Mol. Biol.* **865**, 193–206 (2012).
11. Perez, D. R., Seibert, B., Ferreri, L., Lee, C.-W. & Rajao, D. Plasmid-Based Reverse Genetics of Influenza A Virus. *Methods Mol. Biol.* **2123**, 37–59 (2020).
12. Yoneda, M. *et al.* Establishment of a Nipah virus rescue system. *Proc. Natl. Acad. Sci. U. S. A.* **103**, 16508–16513 (2006).
13. Griffin, B. D. *et al.* Establishment of an RNA polymerase II-driven reverse genetics system for Nipah virus strains from Malaysia and Bangladesh. *Sci. Rep.* **9**, 11171 (2019).
14. Tumpey, T. M. *et al.* Characterization of the reconstructed 1918 Spanish influenza pandemic virus. *Science* **310**, 77–80 (2005).
15. Yun, T. *et al.* Efficient reverse genetics reveals genetic determinants of budding and fusogenic differences between Nipah and Hendra viruses and enables real-time monitoring of viral spread in small animal models of henipavirus infection. *J. Virol.* **89**, 1242–1253 (2015).
16. International Gene Synthesis Consortium. <https://genesynthesisconsortium.org/>.
17. O’Neal, A. J. *ChatGPT-Dan-Jailbreak.md*. (Github).
18. Christiano, P. *et al.* Deep reinforcement learning from human preferences. *arXiv [stat.ML]* (2017).
19. Soman Pillai, V., Krishna, G. & Valiya Veetil, M. Nipah Virus: Past Outbreaks and Future Containment. *Viruses* **12**, (2020).
20. Madhav, N. *et al.* *Pandemics: Risks, Impacts, and Mitigation*. (The International Bank for Reconstruction and Development / The World Bank, 2017).
21. Esvelt, K. M. Delay, detect, defend: Preparing for a future in which thousands can release new pandemics. *Geneva Papers* (2022).
22. Lewis, T. The Quest to Overcome Gene Therapy’s Failures. *Nature* (2021) doi:10.1038/d41586-021-02734-w.
23. Bai, Y. *et al.* Constitutional AI: Harmlessness from AI Feedback. *arXiv [cs.CL]* (2022).
24. Bügl, H. *et al.* A Practical Perspective on DNA Synthesis and Biological Security (12/4/2006 Draft). *MIT DSpace* (2006).
25. Diggans, J. & Leproust, E. Next Steps for Access to Safe, Secure DNA Synthesis. *Front Bioeng Biotechnol* **7**, 86 (2019).
26. Grange, Z. L. *et al.* Ranking the risk of animal-to-human spillover for newly discovered viruses. *Proc. Natl. Acad. Sci. U. S. A.* **118**, (2021).
27. Warren, C. J. *et al.* Primate hemorrhagic fever-causing arteriviruses are poised for spillover to humans. *Cell* **185**, 3980–3991.e18 (2022).
28. Gretton D, Wang B, Foner L, DeBenedictis EA, Liu AB, Chory E, Cui H, Li X, Dong J, Fabrega A, Dennison C, Don O, Tong Y, Uberoy K, Rivest R, Gao M, Yu Y, Baum C, Damgard I, Yao AC, Esvelt KM. Random adversarial threshold search enables specific, secure, and automated DNA synthesis screening. *SecureDNA project*.
29. Kang, D. *et al.* Exploiting Programmatic Behavior of LLMs: Dual-Use Through Standard Security Attacks. *arXiv [cs.CR]* (2023).
30. Baum C, Cui H, Damgard I, Esvelt KM, Gao M, Gretton D, Paneth O, Rivest R, Vaikuntanathan V, Wichs D, Yao A, Yu Y. Cryptographic Aspects of DNA Synthesis Screening. Preprint at (2020).

The CHAIRMAN. Scientific and engineering expertise has long been a barrier that protects us from rogue actors. Until now, the common person has not had access to the resources or the know-how to launch these high-tech threats on human society. Irresponsible availability of AI technologies risks eliminating much of the expertise required to develop a weapon, disease, or cyberattack, thereby eroding defenses we had in the past. AI is not a new issue for the Committee or the Department of Energy. Since the 1960s, DOE has been a key player in investments in AI and automated reasoning. As we all know well, the Department has 17 national labs and 34 user facilities that are crown jewels of America's R&D network. DOE's national laboratory system houses a workforce of over 70,000 scientists, engineers, researchers, and support personnel with world-leading scientific expertise, whose mission is to serve the American people. Each of these labs plays a significant role in the future of AI.

As I mentioned earlier, DOE is also the largest funder of the physical sciences and manages more scientific data than any other agency in the U.S. As a result, the Department has computing resources, expertise, and experience in managing large volumes of data that give the Department their natural leadership on artificial intelligence. When federal agencies have an AI problem, they look to the DOE and its labs for help. Over the past decade, the Department has developed thousands—and I say thousands—of AI applications. For example, the National Energy Technology Lab in Morgantown, West Virginia—my home area—supports the Department of the Interior in using artificial intelligence to identify orphan oil and gas wells. For the orphan well program, AI serves resources by analyzing old land survey maps, drilling permits, historical images, production records, and eyewitness accounts to find well sites.

During the 2023 R&D awards, which I am told is referred to as the "Oscars of Innovation," Dr. Rick Stevens, of Argonne National Lab, who is one of our witnesses today, was recognized for his work using AI to accelerate the discovery of new cancer therapies and treatments that are highly personalized for individual patients. And our Committee has recently played an important role in advancing DOE's AI work. Recognizing that the United States must not fall behind in the supercomputing race, we authorized the Exascale Computing Project at the Department of Energy in the 115th Congress. In May of last year, the Frontier supercomputer at Oak Ridge National Laboratory in Tennessee passed exascale—the ability to perform one billion—billion—calculations per second—that's a lot—making this the fastest supercomputer in the world. Before we authorized the Exascale Computing Project, China had the fastest computers. Now, the U.S. has regained the lead. This supercomputer at Oak Ridge is already using AI to model the behavior of human cells to develop better treatments for Alzheimer's, opioid addiction, and cancer.

But the global AI race is just beginning. AI has the potential to add trillions of dollars into the world economy each year. Governments and companies around the world are competing fiercely in the new market. In particular, America must accelerate our efforts to compete and defend against China on AI. It is estimated that the annual Chinese AI investments will reach over \$26 billion by

2026, which dwarfs the U.S. government's current spending of about \$3.3 billion per year.

Between 2015 and 2021, Chinese AI companies raised \$110 billion, including \$40.2 billion from U.S. investors, which I cannot even believe, in 251 AI companies. In 2017, China released their "New Generation of AI Development Plan," which includes R&D and infrastructure targets. The U.S. currently does not have a strategic AI plan like this. In addition to government spending, China's workforce advantage is significant. It has twice as many STEM Ph.D.s and twice as many STEM master's degree holders than the U.S. China has created artificial intelligence Ph.D. programs in every one of their top universities.

In regards to the Exascale Computing Project this Committee championed, the Chinese government could be set to operate as many as ten—as many as ten—exascale supercomputers by 2025. Xi Jinping himself has pointed to our national lab network, calling them "indispensable momentum for the development and innovation of science and technology." Soon, China may have their very own lab network. Just last week, a company named Baidu released "Ernie Bot," which is a Chinese Communist Party-approved AI language model comparable to "ChatGPT," an app developed in the U.S., which we have all heard a lot about. "Ernie Bot" is the most downloaded app in all of Asia and is expected to continue to grow.

It is clear to me that DOE needs to do more strategic planning around AI so that Americans have confidence that we are leveraging our key resources, such as our national labs, to their fullest potential. We should encourage other agencies to use DOE's AI resources and promote private-sector partnerships with the Department and the national labs to develop safe commercial applications of AI. We must also understand what additional investments are needed to spur U.S. leadership in artificial intelligence. Congress should focus on strengthening and expanding our impressive existing programs rather than creating duplicate new programs at other agencies. We should also ensure DOE and the national labs are able to responsibly recruit leading AI experts, both from our country and globally. Much of America's AI expertise comes from abroad. Immigrants founded or co-founded nearly half of top startups in the U.S., and international students earn 60 percent of our computer science doctorates.

All at the same time, we must be absolutely sure that the Department's AI work includes strong research security requirements. We will not outcompete China in AI if they are able to just steal the technology funded by our taxpayers' dollars. The CHIPS and Science Act that passed last Congress featured research security improvements that are now law and currently being implemented by the Department. However, foreign espionage is an evolving threat, and we must remain vigilant and clear-eyed in this threat. The United States must remain at the forefront of new emerging technologies, and the Department of Energy is a central component of that effort.

I am looking forward to hearing our witnesses' perspectives on specific steps our Committee and the Department could take to ensure America is advancing AI in a competitive, responsible manner.

With that, I will turn to my friend, Senator Barrasso, for his opening remarks.

**OPENING STATEMENT OF HON. JOHN BARRASSO,
U.S. SENATOR FROM WYOMING**

Senator BARRASSO. Well, thanks so much, Mr. Chairman, and I appreciate your opening remarks because artificial intelligence is rapidly transforming the world. It is already impacting our daily lives.

Artificial intelligence plays an important role in the energy sector. In mining, AI can reduce equipment downtime. Advanced algorithms help miners locate mineral-rich deposits for more efficient exploration. Real-time analytics strengthen worker safety programs by predicting potential hazards. Artificial intelligence helps pinpoint oil and gas reserves. Predictive models harness data to streamline operations and reduce costs. AI-enhanced sensors also reinforce pipeline safety and efficiency. So artificial intelligence has great promise to expand our economy and to strengthen our national security.

It also raises, Mr. Chairman, as you point out, some well-documented concerns. A recent study at the University of East Anglia highlighted a significant and systemic left-wing bias in the ChatGPT platform. In the United States, it revealed a clear bias in favor of Democrats. The same program favored the Labor Party in the United Kingdom and the Workers' Party in Brazil. We can't let political bias infiltrate development of AI. This is particularly true when taxpayer dollars are helping fund the technology's development.

Innovation in emerging technologies like artificial intelligence can be a source of great strength. It can be a key advantage in our geopolitical competition, as you point out, Mr. Chairman, with China and with Russia. It can also create a national security risk if the technologies are not properly protected. The Department of Energy has an important role in artificial intelligence research. The Department maintains the world's most advanced computing systems. Its 17 national labs have significant experience developing our nation's most sensitive technologies.

For this reason, the People's Republic of China is watching nearly every move that is made at our national labs. A recent report revealed that since 1987, the Chinese Communist Party has targeted over 160 Chinese researchers working at our premier nuclear weapons lab. Upon returning to China, these researchers help to advance key military technologies using knowledge financed by American taxpayers. In July of this year, senior FBI officials warned that China is targeting U.S. businesses, universities, and government research facilities. China is trying to get their hands on cutting-edge American research and technology. As of 2021, over 4,000 non-U.S. resident Chinese nationals still work at our nation's labs—at the national labs. Many of these foreign nationals strive to further scientific innovation and do want to collaborate in good faith. They find themselves beholden to an authoritarian regime at home, and the Chinese Communist Party is relentless. Some of these Chinese nationals will see no choice but to support the Chinese Communists through theft of research and technology. Their

families back in China may suffer harsh consequences if they do not comply with their government's demands.

China's sustained interest in our intellectual property is a stark reminder of the intense global competition surrounding artificial intelligence. This competition may drive advancements in the field. We can't overlook the threat to our economic and national security posed by the Chinese government. The Department of Energy and our national labs must take the China threat more seriously. We can't let our technology fall into the hands of those in Beijing.

I look forward to hearing from our witnesses today on what additional steps research agencies and the laboratories and the universities that they fund must take to prevent this theft of American technology.

Mr. Chairman, thanks for calling this important hearing.

The CHAIRMAN. Thank you, Senator.

I would like to first of all thank the witnesses for being here today and I appreciate very much you all coming and making the effort.

First of all, we are going to have David Turk, Deputy Secretary of Energy.

We have Dr. Rick Stevens, who I mentioned before, and thank you for the great work and being recognized for that, Associate Laboratory Director of Argonne National Laboratory.

Ms. Anna Puglisi, Senior Fellow, Georgetown University Center for Security and Emerging Technology.

And Mr. Andrew Wheeler, Vice President and Fellow at Hewlett Packard Enterprise.

And again, thank you all.

I will turn to Deputy Secretary Turk. We are going to begin with your opening remarks.

**STATEMENT OF HON. DAVID M. TURK,
DEPUTY SECRETARY, U.S. DEPARTMENT OF ENERGY**

Mr. TURK. Chairman Manchin, Ranking Member Barrasso, distinguished members of the Committee, thank you for the opportunity on behalf of the Department of Energy to talk about our activities in and our vision for artificial intelligence. Let me begin, appropriately so, by thanking this Committee for years and years of strong, sustained support that has led to the DOE becoming an AI powerhouse. And Chairman, you laid out much of that in your own opening statement. With your leadership, we have designed, developed, and currently operate four of the top ten fastest openly benchmarked supercomputers in the world, including, as the Chairman mentioned, the world's fastest—Frontier—at Oak Ridge National Lab.

Through the Exascale Computing Project, DOE is developing the world's first capable exascale software ecosystem that is helping to drive breakthroughs—AI breakthroughs—in critical areas as varied as materials science, cancer research, earthquake risk assessment, energy production and storage, computational weapons applications, and I could go on and on. Across a network of 34 national user facilities around our country, DOE generates tremendous volumes of high-quality data, literally the fuel that can lead to more AI breakthroughs. And most importantly, DOE's national labora-

tory system houses a workforce of over 70,000 scientists, engineers, researchers, and support personnel with world-leading expertise.

It is a particular pleasure to be joined on this panel by Professor Rick Stevens, who is one of those top experts, as you mentioned, Chairman, in your opening statement. But as proud as we all should be about this robust AI foundation at DOE, now is the time to take these capabilities to the next level. Advances in AI are enabling enormous progress and breakthroughs that can help address key challenges of our time. And we need to double down on that technical capability—the computers, the software, the data, and most importantly, the researchers, to make sure that we have those breakthroughs here in the U.S., and our private sector can benefit from that as well.

Governments around the world are investing in AI capabilities as never before. Chinese investments are expected to reach, as the Chairman said, over \$26 billion by 2026. We simply must be bolder and move faster or risk falling behind. AI also lowers the bar for bad actors to do even worse things and to do those worse things easier. AI systems can pose risks to individual safety, privacy, and civil liberties, risks to society for information manipulation, as the Ranking Member stated, bias and discrimination, social engineering, and market manipulation, biothreats, nuclear threats, chemical threats—all made easier by AI, potentially. An industry alone cannot be fully aware of the relevant risks and threats because much of that information, rightfully so, falls within the purview of our intelligence community and our national security enterprise.

DOE can play an incredibly important role here, including developing methods for assessing and red teaming AI models to identify and mitigate the risks presented by these cutting-edge AI systems that are only developing, and improving incredibly quickly over weeks and months ahead. Over the past five years, we have worked with stakeholders across the AI ecosystem to identify new and rapidly emerging opportunities and challenges presented by AI, and to identify very specifically how unique DOE capabilities—the strong foundation, again, thanks to this Committee—how we can drive progress for AI going forward from the Department of Energy side of things. This culminated in the May 2023 release of a report called “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. We have translated this feedback into a specific proposal for your consideration called “The Frontiers in Artificial Intelligence for Science, Security, and Technology,” or FASST, by acronym. This is exactly, Chairman, as you said, a strategic vision, a strategic plan for the DOE nested within a broader strategic vision for the U.S. and the U.S. Government.

Mr. Ranking Member, you rightfully point out that there are also research security issues and challenges we need to take head-on and be eyes-wide-open and improving our systems on a regular basis. I want to thank our fellow panelist, Ms. Puglisi, for her testimony, for all her work—excellent testimony that we can improve on even further on the Department of Energy side, including our science and technology risk matrix, which I would be happy to get into in the question-and-answer session. We look very forward to

further discussing the FASST proposal, everything else we are doing, and updating it based on this Committee's continued guidance and leadership. There is no doubt that with AI we are now on the cusp of our next grand challenge here in the United States. Working within and outside the government, DOE stands ready to step up to this moment, to play our role in fully engaging in this grand challenge by utilizing our unique computing capacity, comprehensive, well-curated datasets, our algorithms, relationships with industry, and again, most importantly, our skilled, leading scientific workforce. All of us at the Department of Energy and our national labs very much look forward to working with this Committee to live up to this moment.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Turk follows:]

TESTIMONY OF DEPUTY SECRETARY DAVID TURK
U.S. DEPARTMENT OF ENERGY
BEFORE THE
COMMITTEE ON ENERGY AND NATURAL RESOURCES
UNITED STATES SENATE
REGARDING
ARTIFICIAL INTELLIGENCE
SEPTEMBER 7, 2023

Introduction

Chairman Manchin, Ranking Member Barrasso, 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 carries 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 present for the Committee's consideration a vision for how DOE can play our role within a broader U.S. strategy 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 and sustained investments in DOE for many years that have enabled DOE's existing infrastructure and capabilities for cutting-edge AI. These extensive investments 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.
- **Advanced software:** DOE has created a wealth of science and engineering algorithms that can run on the most advanced supercomputers, and through 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 materials science, AI, cancer research, earthquake risk assessment, energy production and storage, and computational weapons 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.
- **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; 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:

- *Assisting in emergency response:* Researchers at DOE's Pacific Northwest National Lab used their AI-based image analytics and model to assist the Coast Guard with modeling fire spread and evacuation efforts in Maui.
- *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.
- *Enhancing efficiency and safety:* Today, we are already utilizing AI to help determine the condition of oil and gas wellheads, making it safer and more efficient for human operators to do their jobs.
- *Protecting our electric grid.* DOE has developed an edge machine learning model that was deployed on a microprocessor card to detect gunshots to enable physical protection of our electric grid.

Nuclear Security and Nonproliferation:

- *Nuclear nonproliferation and nuclear security:* National Nuclear Security Administration (NNSA) laboratories are pursuing research in foundation models for nuclear nonproliferation and nuclear security applications in HPC, cloud, and hybrid environments, making inroads in test and evaluation, and addressing transparency, usability, and robustness in human-AI teaming.
- *New materials discovery:* DOE is using AI and machine learning (ML) methods to enhance and extend pit production, additive manufacturing of new components, component/system surveillance, design of new experiments, and proliferation detection. 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, uncovered key interactions among new materials, and revealed deep fakes.
- *Understanding the battlefield of the future:* NNSA is also utilizing computing and algorithmic innovations to improve dynamic decision support - from better understanding the battlefield of the future to discovering and countering novel proliferation pathways. DOE will also 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 to develop safeguards that can be implemented to prevent AI from aiding malevolent actors.

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/NNSA's development and application of these novel AI methods.
- *Understanding the evolution of the virus behind COVID-19:* A team from Argonne National Laboratory that included academic institutions and hardware companies developed 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.

Promising opportunities

AI is a powerful technology that presents breathtaking opportunities for our nation, and the Biden-Harris Administration is taking steps 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.

Over the next few years, AI has the potential to help transform the way we utilize the grid and deploy clean energy technology. The deployment of new technologies such as wind, solar, energy storage, electric vehicles, controllable building loads, and other smart grid devices increases the complexity of energy system planning and operations by orders of magnitude, and utilities across the country are struggling to keep up with these changes. AI-enabled modernization of our nation's integrated electricity delivery system can help speed up deployment to provide energy to every last community and simultaneously achieve affordability, carbon neutrality, reliability, and resilience to extreme (both natural and intentional) events. DOE and our labs can serve as a platform for dealing with proprietary data to help with real-time energy decision-making – from where renewables should be sited to where utilities should harden the grid.

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. AI can help speed the discovery of novel materials, counter proliferation pathways, and help us develop real-time and predictive understanding of the battlefield of the future.

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

Oceanic and Atmospheric Administration (NOAA) to use supercomputers for earth system modeling, supporting sub-seasonal to decadal earth systems forecasts, and DOE is collaborating with the National Cancer Institute to develop new computing tools that integrate novel AI and uncertainty quantification technology and take advantage of DOE's advances in computing—including Frontier, the Nation's first exascale computer—to accelerate discovery in cancer research.

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 and leveraging guidance from the AI Risk Management Framework and the Blueprint for an AI Bill of Rights, in order to better inform Federal AI policy.

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, with investments expected to reach nearly \$27 billion by 2026. 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 strong 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.

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.

Unless the US government and industry take action now, we could easily find ourselves faced with technological surprise driven by those who do not share our values or being unable to respond to the unanticipated consequences of a rapidly changing technological landscape.

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 priorities on AI 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 of AI.

Leadership in AI means outpacing the competition in AI development and deployment. This means AI-enabled accelerated science and technology innovation, using AI to create more efficient and equitable services in both the private and public sectors in a manner that increases trust in our institutions, and it means living in a world where we mitigate risks from AI effectively so everyone can enjoy the benefits of AI.

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 this Committee's 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 emerge constantly, often 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 represent the global stakes for AI competitiveness, but leadership will hinge on developing sustainable exascale and beyond-exascale (zettascale) 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. For example, we are already working to understand the implications of these new capabilities as they relate to nuclear security challenges by integrating our authoritative knowledge of nuclear weapons to understand how AI can shorten a proliferant nation's nuclear weapon development time frame.

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 2023, the second DOE exascale machine will provide twice this capacity.

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. One NNSA lab is developing a federated data management system for all of its data, which would operate across multiple classification data fabrics, enable colocation of data with

compute resources, both high performance computing and cloud, and integrate with other government data management systems to enable transformative research in nuclear nonproliferation and nuclear security.

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.

We can leverage DOE's existing broad technical expertise, world-leading computing capabilities, and industry partnerships, to develop next-generation AI systems to advance and further democratize science and technology development, thus enabling our clean energy future and ensuring science and technology leadership for the nation. Working with other departments and agencies, we can enable trustworthy AI development and deployment across the government and the private sector, create more efficient and equitable services and reduce regulatory compliance burdens while providing better customer service and more-transparent actions in a manner that increases trust in our institutions.

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 must act urgently to 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.

The CHAIRMAN. Thank you, Deputy Secretary Turk.
And now we are going to go to Dr. Stevens.

STATEMENT OF DR. RICK L. STEVENS, ASSOCIATE LABORATORY DIRECTOR, COMPUTING, ENVIRONMENT, AND LIFE SCIENCES, ARGONNE NATIONAL LABORATORY

Dr. STEVENS. Thank you, Chairman Manchin, Ranking Member Barrasso, and members of the Committee for this opportunity to participate in today's discussion about national labs and AI. I have worked on advanced computing for over 30 years at Argonne and at the University of Chicago, and for much of that time, I have been driven by this idea that we need to build intelligence into future computing. And over the last four years, I had the fortune to work with my colleagues at all the labs—all 17 labs, over 30 universities, and dozens of companies to run a series of town hall meetings—seven town hall meetings over four years—that involved over 1,300 researchers. And at these meetings, we challenged the community to think broadly about how advanced AI systems, going beyond what we can do today, could be developed and applied in DOE mission spaces to accelerate scientific research, accelerate development of energy technologies, and improve national security-related work. And what I am going to tell you about right now is a little bit of those outcomes of that report.

The consensus is that there is an enormous opportunity here to use AI to accelerate discovery both in basic science, accelerate the application of that in energy technologies, and to improve how we actually conduct all of our work in national security. Some of these applications could range from new technologies for better batteries that, say, require less rare-earth minerals, which would improve global security in and of itself, to new types of polymers that could be ideal for each application but could be recycled indefinitely without losing performance. We don't know how to do that today, but we think AI could help us with that. We believe AI could be coupled with robotics to automate much of experimental science, improving throughput by orders of magnitude. In fact, it is so compelling, that idea that some of my colleagues have formed, this concept of AI-driven science factories, or some people call it self-driving laboratories, as a way that we will actually accelerate work in drug development for cancer or new materials for semiconductors.

AI can also address key challenges in software development. DOE manages over billions of lines of code, and we do not have enough developers, enough senior software developers to maintain that code and deport that code to new machines. We know AI can help us with that problem. In fact, AI systems appropriately trained and tuned could help us design not only software, but hardware for next-generation systems and help us build systems that could save a huge amount of energy. AI systems are also being used to explore ways to control complex systems, like fusion reactors. And we think that same idea could be applied to control future power grids where we have a diversity of sources and changes in demand. AI can also be used to accelerate scientific simulations by replacing traditional numerical methods with new AI-driven methods in achieving speedups of factors of 100 or more across

many applications, from weather prediction, to electronic structure computation that is used on over 30 percent of DOE computers.

And finally, the biggest opportunity is probably this idea of foundation models—the underlying technology behind things like ChatGPT, but applying that to science. We are discovering that those types of technologies are incredibly versatile for doing scientific problems. They have been trained on millions of science papers—vastly more knowledge than individual scientists would ever absorb in their lifetime, and can be used to integrate and synthesize knowledge, suggest new lines of attack on open problems and so forth. In short, and as a surprise to many, current foundation models have demonstrated an unusual utility in science maybe a decade earlier than we thought. And that is one of the dramatic opportunities and challenges because these models can directly affect scientific productivity today, and we do not have a strategy across the Department for aggressively using this. It is a big, big opportunity and also a challenge.

So AI, in all of its forms, is rapidly becoming the most important tool in the scientific and technical toolbox. And as a result of these workshops and the progress over the last five years, I believe it is imperative that the U.S. lead the world in the development of advanced AI systems for scientific and national security applications. I believe DOE is the only agency that can do this, that has all the resources under one roof. Of course, it's going to be a partnership with private industry to do this, and with our academic colleagues. I believe we should commit over the next decade to building the most powerful advanced AI capability for science, energy, and national security. Some might call it an artificial general intelligence for science, or perhaps a super-intelligence for science. It could have many names, but the goal is to go dramatically beyond where we are today in a secure fashion and a reliable fashion.

Whoever leads the world in AI for science will lead the world in scientific discovery and have a head start in the translation of those discoveries into products that expand our economy and address modern needs. And in doing that, we will secure what I call the innovation frontier by AI. Whoever leads the world in the development of AI for energy will lead the world in developing and deploying next-generation energy technologies, such as modular reactors that can be safe and deployed anywhere at a moment's notice, or super-efficient combustion systems to take maximum advantage of our resources, and scalable approaches to carbon sequestration, which we desperately need, and better and more effective strategies for electrification of the economy. And by doing that, we will secure the energy and climate frontier. And finally, whoever leads the world in understanding and mitigating the risks of AI and the use of AI to improve national and global security will determine the landscape in which we and our allies will live and work in the future, securing our lifestyles and our prosperity.

Thank you for your time, and I really look forward to the questions.

[The prepared statement of Dr. Stevens follows:]

Testimony of Rick Stevens
Associate Laboratory Director for Computing, Environment, and Life Sciences
Argonne National Laboratory

Senate Energy & Natural Resources 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

September 7, 2023

Chairman Manchin, Ranking Member Barrasso, and Members of the Committee, thank you for the opportunity to participate in today's discussion about the important role the Department of Energy (DOE) and its national laboratories have in advancing a national, trustworthy, reliable artificial intelligence (AI) capability that will accelerate science, transform innovation, and underpin our future economic and national security.

I am Rick Stevens, the Associate Laboratory Director responsible for Computing, Environment, and Life Sciences research at Argonne National Laboratory and a Professor of Computer Science at the University of Chicago. For over 30 years, my work at Argonne has focused on advancing computer science to tackle grand challenges across many science domains, from fusion energy to medicine. I have helped develop ever-more-powerful generations of supercomputers, culminating in the current generation of exascale supercomputers that are coming online now.

Over the last four years, I have had the fortune to work with my colleagues at the DOE laboratories to organize seven "town hall" meetings on the use of AI to advance science, energy, and national security. Over 1,300 scientists and engineers from all 17 national laboratories, more than 30 universities, and dozens of companies participated. In these meetings we collectively thought broadly and aggressively about how advanced AI systems might be developed over the next ten years to accelerate scientific research, energy technology development, and improve national security.

What has become clear as a result of these town hall meetings and the progress we have made in AI research at the national labs, combined with the speed with which AI tools like ChatGPT are being adopted by the public, is that *AI will completely transform science and society*.

AI is in the same class of transformative technologies as electricity and computers. Both were revolutionary, although they weren't necessarily recognized as such at the beginning. And the beginning is where we are with AI today.

Like all transformative technologies, there are both immense opportunities and risks associated with widespread use of AI. I believe it is imperative that the United States lead the world in the development of advanced AI systems for scientific and national security applications, and that an effort on the scale of the Manhattan Project will be needed for us to do so. I appreciate the

opportunity today to highlight the opportunities and risks associated with AI, and outline how the national labs and DOE are uniquely positioned to build an advanced AI capability for the nation.

The opportunities of AI for science and national security—and the risks

AI is a tool for the mind. An amplifier of thought, a super-smart assistant, and perhaps someday soon, a powerful concierge for nearly all aspects of life and work. Unlike the internet, which enables humans to find information, communicate with each other, and transact business, AI is much more.

Trained on ever-larger ensembles of human and machine-generated knowledge, AI is capable of integrating and synthesizing knowledge and carrying out self-directed sequences of steps to solve problems in response to human prompts or questions.

Generative AI large-language models (LLMs)—such as Open AI’s ChatGPT, Google’s Bard, Anthropic’s Claude2 and other generative systems for images, music, speech, and computer code—have made AI widely available to the public. These new AI interfaces are immensely popular. ChatGPT gained 1 million users in five days and 100 million in two months, making it one of the fastest technologies ever to be adopted. We are seeing the beginning of a vast transformation of how people will work with, and interact with, computers and the internet.

Imagine a world where every person has 24/7 access to an incredibly smart assistant that has been trained on the sum of human knowledge. Your AI assistant will know a hundred human languages, all recorded history and literature, the bible in Hebrew and Greek, non-classified and non-proprietary science and engineering, political theory, military tactics and strategy, popular culture, the locations and relationships between companies, and much more.

You will no longer have to search the internet to find information and read through the resulting pages to synthesize answers. With AI assistants, you pose a query (much like we talk or text today), and the AI assistant does the searching and synthesizing. It writes the paper, answers the questions in your homework, plans your vacations, writes the employee evaluation, summarizes the financial market, or writes your computer code. In the future, we can even envision an AI that’s perceptive enough to ask questions before you realize you have them, just by listening or watching.

AI is beginning to transform some science and technology fields. AI systems are already being used to explore ways to improve the control of nuclear fusion reactors, increasing stable plasma burn times, and dynamically adjusting controls to avoid plasma disruptions. AI is also being used to accelerate scientific simulations by augmenting and/or replacing the traditional numerical mathematics approaches, in some cases providing massive speedups on existing computer hardware. Early efforts have achieved factors of 100 or more for problems such as molecular electronic structure and weather prediction, but many more areas are ripe for exploration. AI models are already writing code and will soon excel at it, even for quantum computers.

There are enormous opportunities for AI to accelerate discovery in the basic sciences, from new materials for energy applications such as better batteries that require less rare earth minerals, to new types of polymers that are optimal for each application yet can be reprocessed and recycled without loss of performance.

AI coupled with robotics can be used to improve throughput for experimental science many orders of magnitude, leading some to imagine future AI driven “science factories” that could be used to solve problems in many domains, from developing new drugs for infectious diseases and cancer to exploring new types of semiconductors.

AI can also address key challenges in software development, from improving the productivity of programmers for scientific computing, to optimizing performance of codes for our supercomputers. This is important to DOE and the national labs since we maintain over 10 billion lines of code in our laboratories, and it will also be critical for the computing industry.

Trained and tuned AI systems will be able to help us design better and more energy-efficient chips for future supercomputers and optimize the hundreds of processing steps used to manufacture chips in US-based semiconductor factories. AI-based control systems will improve the reliability and stability of the electrical grid, by adjusting operating controls quickly and precisely to balance increasing diversity of energy sources and changes in demand.

AI will improve overall scientific and technical productivity, in some cases speeding science discovery up by 10 times or more. And it will also change the nature of how science is conducted, with AI assistants playing important roles as sounding boards for new ideas and as planners and doers for experiments.

On the cautionary side, AI will pose new risks and threats. As an amplifier of human skills and capabilities, AI has the ability to greatly speed scientific discovery and improve productivity, and it can be used for good and bad purposes. To date, most AI efforts undertaken by industry and other countries have been generally visible, and the scientific community becomes aware quickly when new models are created. In the future, some AI models will be built by large groups working together largely in the open, while others will be built in secret. A small group working in secret with sufficiently powerful AI tools could develop a novel chemical, biological, or cyber threat. We will need to transform how we manage the risks posed by bad actors using the same AI tools we are using to improve science and advance society.

We also need to recognize the fierce international competition that is already underway to build the most capable AI systems. Powerful AI models are already emerging around the globe, including Falcon from Abu Dhabi. In China, hard numbers for public investment in AI are difficult to obtain, but they are estimated at \$2-\$9 billion a year now, up to \$26 billion by 2026. My other colleagues on the panel could expand upon the competition with China in much more detail. Whoever leads the world in AI will lead in science, innovation, energy, and security, and other countries are already positioning themselves for the competition.

The time is now for our country to take the lead in this race, and we believe DOE and the national laboratories have an integral role to play.

Why build specialized AI systems for science, energy, and security?

One could ask why the government or DOE need to develop their own AI capability. Why not just use commercial AI systems like GPT-4 to do the same work?

I believe that researchers should be using commercial AI systems as much as possible, when they are the best tool and when the open nature of their use is not a problem. As commercial AI companies develop and deploy enterprise versions that have more protections of user data, these models should be adopted for use in appropriate settings.

However, we need to go beyond commercial systems in these important ways.

- 1) **Specialized data.** Commercial systems will never be deeply trained on the vast quantities and diverse types of data that are currently being managed by DOE laboratories. DOE has thousands of times more scientific data than the largest AI models are currently trained on. This data comes from experiments and from computer simulations and spans dozens of scientific fields. The scientific community needs AI systems that deeply understand scientific data, scientific processes, and scientific reasoning. DOE needs AI systems that have mission-related datasets. For national security applications, DOE needs models that can operate on that type of data in a classified environment.
- 2) **Trust and reliability.** Many of our use cases for AI (scientific data analysis, mission-critical decisions, operations of complex and life-critical systems) require high levels of accuracy in predictions. They also require reliable models whose training data is known, and whose outputs can be trusted and validated at scale.
- 3) **Security.** Whether for national security applications or sensitive science (such as understanding the risks posed by third-party models) we need to have the most powerful AI models in secure enclaves where they can be developed, used, and evaluated. An important class of uses of advanced AI will be to manage, control, and analyze experiments and large-scale simulations. In these roles the AI will need to be tightly integrated with robotic laboratories and supercomputing infrastructures, often in complex and secure environments.

Building the most advanced AI systems is truly a large-scale activity

The DOE national laboratories were founded out of the Manhattan Project—our nation's first example of leveraging teams of thousands of scientists and engineers, stationed at centers across the country, to accomplish a Herculean scientific endeavor in a very short period of time.

State-of-the-art AI systems are difficult to build, requiring millions of dollars of computing time and large teams of researchers that only exist in relatively few institutions. Building an advanced AI capability for science, energy, and national security—and doing it before, and better than, other countries—will require a project of similar scale and investment as the Manhattan Project.

World-leading AI research groups operate at the scale of 1,000 researchers and developers working on a small number of models and systems. Even at this scale, with access to sufficient computing power and large-scale data, these teams produce a major model system on an annual or biannual pace. It is not unusual to take months to initially train a model, many more months to refine the model and to evaluate it and improve its safety and alignment, and many more months after that to produce versions for specific purposes. Once models are developed, they must be deployed and refined as they ramp up usage and become integrated into the production environment.

We expect that DOE national labs will be a primary developer of AI models for scientific and national security uses. Some models developed by DOE laboratories will be widely used by the scientific community, perhaps hosted by laboratories or in partnership with companies. Others will be deployed in secure environments. A single foundational science model could be deployed for hundreds or thousands of downstream applications, and derivative models could be produced for even more.

As a trusted neutral party, DOE can also play a major role in development of the science of “AI risk management,” especially when it involves assessing the risks of third-party models using scalable methods (i.e., using AI systems and large-scale computing to automate as much of risk assessment as possible). By partnering with other agencies and leveraging its expertise in scalable computing, DOE can play a major role in developing the technical means for AI risk assessment and determining fitness for purpose. These techniques could be made available to regulators with responsibility for AI regulation and assessment.

A possible model for a national AI project for science, energy, and national security

A new initiative by DOE and the national laboratories could be created to position the United States as the undisputed leader in AI research, development, and deployment for science, energy, and national security.

Through a committed partnership between the DOE’s Office of Science, the DOE National Nuclear Security Administration, and the DOE’s applied energy programs, a coordinated effort could build the world’s most powerful AI systems explicitly targeting accelerating scientific research and technology development. This AI leadership would be enabled by harnessing the DOE’s exascale computing resources and its integrated data and research infrastructure supporting the world’s largest collection of national user facilities and collections of scientific

data. This capability could allow DOE to bring AI research challenges via the largest scientific and mathematics workforce under one organization.

A network of groundbreaking AI research clusters could be established, built on DOE's unparalleled ecosystem of high-performance computing capabilities and research facilities. This network would operate as public-private partnerships, fusing the expertise and perspectives of national labs, academia, and industry leaders. It would also tap into the thousands of scientists, mathematicians, and engineers within the DOE lab complex to tackle multifaceted challenges requiring integrated, multidisciplinary thinking. By bringing together interdisciplinary teams, innovation cycles would be accelerated, ideas rapidly translated into deployable solutions, and insights and models broadly shared across institutional boundaries.

A primary research goal for this national effort would be pioneering advanced AI techniques for science and engineering tasks that push beyond human reasoning and learning capabilities. Progress in this direction would enable AI systems to flexibly adapt to novel contexts and tasks by building causal, intuitive understandings of the world. These advanced AI systems would become key assistants and autonomous tools for accelerating scientific research.

The effort would also emphasize developing responsible and trustworthy AI that balances robust performance with safety and security. This involves mathematical methods, software frameworks, datasets, and testing protocols to ensure model fairness, interpretability, reliability, and integrity. AI systems would be designed with transparency, auditability, and human oversight in mind from the start. The program would additionally support fundamental research into AI safety, aiming at avoiding harmful behaviors in future advanced systems.

The effort's scale and visibility could position DOE to lead national and global conversations on managing risks posed by ever-improving AI models. DOE and national lab researchers would collaborate with academic, industry, and government partners to pioneer frameworks and best practices for addressing AI risks to individuals and groups. The effort would work to establish international norms and deterrents for global risks from potential adversarial uses of advanced AI.

The effort would target developing world-class AI-enabling technologies to amplify returns on investment in fundamental AI research. Future AI systems will require advances in parallel computing hardware and software, new algorithms to make training and evaluation more data efficient and advances in data-oriented computing methods.

Science-focused AI systems would accelerate discovery and optimization across disciplines like materials science, particle physics, molecular biology, chemistry, and environmental sciences. Advanced software libraries, execution frameworks, high-performance workflows and cloud-based development environments will lower barriers to applying AI techniques. Specialized AI hardware architectures and low-power processing units will enable deploying high-performance AI affordably at scale.

DOE's unparalleled national lab network and high-performance computing resources will combine to create an integrated data and experimentation ecosystem. By pooling the exabytes of observational data, experimental results, and simulation output datasets into curated repositories with common standards, AI training and discovery would be empowered at a scale exceeding any academic or industrial counterpart. Tight integration of edge devices, high-speed networks, and cloud compute resources will support efficient distributed workflows.

Industrial partnerships and investments in AI hardware research and testbeds—aimed at achieving 100-fold improvements in performance per watt over ten years—would continuously improve AI hardware optimized for performance, scalability, cost efficiency, and sustainability. These solutions would expand access to capable AI resources across public and private sectors.

Partnerships with universities and other agencies would expand, deepen, and improve the diversity of the AI workforce, with a special emphasis on the AI for science and engineering uses and the connection of AI to the high-performance computing and modeling and simulation community.

Finally, this national effort would enable partnerships with other federal agencies through interdisciplinary programs, personnel exchanges, and coordinating strategies. These collaborative efforts will enhance the federal ecosystem's ability to develop and deploy advanced AI systems. This holistic approach would synergize national efforts toward responsible leadership in artificial intelligence.

Conclusion

AI is rapidly becoming the most important tool in the scientific and technical toolbox. It is quite possible that by leveraging sufficiently powerful AI we could make a century's worth of progress in 10 years. I strongly believe that we must explicitly commit to building an advanced AI capability for science, energy, and national security. DOE oversees an unmatched ecosystem of national laboratories and high-performance computing capabilities that together constitute an ideal environment for creating and deploying advanced AI systems.

Whether it is the use of next generation AI models to advance theory in physics, or to synthesize knowledge across scientific literature and databases for a cure for a rare disease, or more specialized AI models exploring novel materials for future microelectronics, three things are clear.

Whoever leads the world in AI for science will lead the world in scientific discovery and will have a head start in the translation of discoveries to products that expand our economy and address modern needs, securing the innovation frontier.

Whoever leads the world in AI for energy will lead the world in developing and deploying next-generation energy technologies such as modular nuclear reactors, super-efficient combustion

systems, new approaches to carbon capture, and new strategies for electrification of the economy, securing the energy and climate frontier.

And finally, whoever leads the world in understanding and mitigating the risks of AI and the use of AI to improve national and global security will determine the landscape in which we and our allies work for the future.

Thank you for your time and careful consideration. I would be happy to answer any questions.

The CHAIRMAN. Thank you, Dr. Stevens.
And now we will have Ms. Puglisi.

**STATEMENT OF ANNA B. PUGLISI, SENIOR FELLOW, CENTER
FOR SECURITY AND EMERGING TECHNOLOGY, GEORGETOWN
UNIVERSITY**

Ms. PUGLISI. Thank you Chairman Manchin, Ranking Member Barrasso, distinguished members of the Committee and staff, and thank you for the opportunity to participate in today's hearing. It is an honor to be here alongside the esteemed experts on this panel. I am currently the senior fellow at the Center for Security and Emerging Technology at Georgetown University. I previously served as the National Counterintelligence Officer for East Asia and have studied China's S&T development and tech acquisition strategy across my career. My testimony today will first address why China targets the DOE labs, provide a brief overview of China's S&T system, and finally discuss potential mitigation strategies. I will also offer lessons learned, which include that this is not a DOE problem, but a U.S.-wide problem, because China's system is not the same as ours.

China takes a holistic approach to developing technology, blurring the lines between public, private, civilian, and military. Our policies and mitigation strategies need to reflect this reality. Beijing, in many ways, understands our societal tensions, and its statecraft is directed at them, exploiting identity politics by promoting any changes in U.S. policy as ethnic profiling. It is because of this last point that I want to acknowledge how difficult and challenging these issues can be. My own grandparents were immigrants who came to this country with little formal education and worked menial jobs. My presence here today is a testament to the American dream. There is no room for xenophobia or ethnic profiling in the U.S. It goes against everything we stand for as a nation. And precisely because of these values, we must move forward to find principled ways to mitigate the policies of a nation-state that is ever more authoritarian and seeks to undermine the global norms of science.

And the importance of science is why China targets the DOE labs. Emerging technologies, as we have heard, such as AI, biotechnology, new materials, and green tech are increasingly at the center of global competition. The DOE labs, because of their mission, are in the crosshairs. While many are familiar with DOE's mission in regards to stewarding our nuclear deterrent, it also plays an essential role in emerging technologies and research, and is essentially a window into the priorities of the U.S. Government. And I have to say, DOE is really an underappreciated resource. While China is not the only country that targets U.S. technology and the DOE complex, China's efforts are complex and multi-faceted and part of a state-sponsored strategy to save time, money, and advance its strategic goals, specifically in these emerging technology areas. My written testimony goes into more detail on the policies, programs, and infrastructure that support these development efforts. China's legal system also complicates collaborations with the DOE complex because its laws compel its citizens to share information and data with Chinese entities if asked, regardless of

the restrictions placed on that data, and more importantly, who owns it. I have also provided these in my written testimony.

Moving forward, we need to consider the following: we need to have policies for the China we have, not the China we want. Most policy measures to date have been tactical and not designed to counter an entire system that is structurally different than our own. It is essential that the United States and other liberal democracies invest in the future. We have heard about the great promise of these technologies, but we must build research security into those funding programs from the start. Existing policies and laws are insufficient to address the level of influence that the CCP exerts in our society, especially in academia and research. Increased reporting requirements for foreign money in our academic and research institutes and clear reporting requirements and rules on participation in foreign talent programs are a good start. We also have to ensure true reciprocity in our collaborations. For too long, we have looked the other way when China has not followed through on the details of the S&T agreements. There have been no repercussions for that, for not sharing data, providing access to its facilities, and obfuscating the true affiliations of its scientists. However, I want to caution—extreme policy reactions, such as closing our eyes and doing nothing, or closing our doors, only really benefit China—the latter by discrediting en masse all efforts to address the problem and by depriving ourselves of the great contributions of foreign-born scientists.

In conclusion, what will also make this difficult is that the reality that China is presenting is inconvenient in the short term. This includes companies looking for short-term profits, academics that benefit personally from funding for their laboratories, and former government officials who cash in as lobbyists for China's state-owned or state-supported companies. I want to thank the Committee again for continuing to discuss this issue. These are hard conversations that we as a nation must have if we want to protect and promote U.S. competitiveness, future developments, and our values. Thank you very much.

[The prepared statement of Ms. Puglisi follows:]

Testimony before the Senate Committee on Energy and Natural Resources on “recent advances in artificial intelligence and the Department of Energy’s role in ensuring U.S. competitiveness and security in emerging technologies”

Anna B. Puglisi
Senior Fellow

Center for Security and Emerging Technology (CSET), Georgetown University
7 September 2023

Chairman Manchin, Ranking Member Barrasso, distinguished members of the Committee and staff, thank you for the opportunity to participate in today’s hearing. It is an honor to be here alongside the esteemed experts on this panel. I am currently a Senior Fellow at the Center for Security and Emerging Technology (CSET) at Georgetown University where I research S&T policy development and global technology competition. I previously served as the National Counterintelligence Officer for East Asia and for most of my career I have studied China’s science and technology (S&T) development and innovation ecosystem, including its efforts to acquire technology and technological know-how, how these efforts have changed over time and the policies and programs China uses to meet its strategic goals.

My testimony today will first address why the DOE labs are targeted by China and the implications of these policies for the U.S.-China strategic competition. I will provide a brief overview of China’s S&T system and finally discuss research security and potential mitigation strategies. In particular, I will discuss how our systems differ, and how the role of the state impacts and influences all aspects of China’s S&T ecosystem, from universities to its state key labs and its associated industries and provide potential mitigation strategies to protect the national innovation base, specifically the DOE complex. Lastly, I’ll offer lessons learned, which include:

- This is not a DOE problem, but a U.S. wide problem because China’s system is not the same as ours. It takes a holistic approach to developing technology—blurring the lines between public, private, civilian and military.
- China says it will use any knowledge or technology it acquires for its military. This is not conjecture, profiling, or analysis, but China’s stated position for decades. Our policies and mitigation strategies need to reflect this reality.
- Scientists—and innovation—thrive with funding, lab space and freedom to pursue their craft—this is what makes the DOE labs such a tremendous resource. Giving scientists a problem to solve is not the same as giving them a solution. Political control is not the same as scientific control. We assume China cannot meet its strategic technical goals because it is not a democracy at our own peril.
- Beijing has made talent development and the exploitation of overseas students, universities, and government labs a central part of its technology acquisition strategy since the country’s “opening” around 1978.¹ This is why the DOE complex is a target.

- Regardless of their personal views, Chinese scientists, businesspeople and officials interacting with the DOE complex have to respond to the PRC's government or security services if they are asked for information or data. China intimidates and harshly silences its critics—this has only grown more so in the past few years. This increasingly includes its citizens abroad.
- Beijing in many ways understands our societal tensions, which include race relations, and its statecraft is directed at them, exploiting identity politics by promoting any changes in U.S. policy as ethnic profiling, offering a narrative about being merely a proponent of “development” and science, in order to divert attention from its own questionable behavior. This is a well-funded effort.ⁱⁱ

It is because of this last point that I want to acknowledge how difficult and challenging discussing these issues can be. My own grandparents were immigrants who came to this country with little formal education, worked menial jobs and made a new life for themselves. My presence here today is a testament to the American Dream. There is no room for xenophobia or ethnic profiling in the United States -- it goes against everything we stand for as a nation.

And precisely because of these values, the issues we are discussing today will make us uncomfortable as we move forward to find principled ways to mitigate the policies of a nation-state that is ever more authoritarian, does not share our values and seeks to undermine the global norms of science and commerce and exploit our national innovation base—especially the DOE labs. These challenges are not about the concerns of one administration or the policies of one political party, but the actions of a nation-state with a different system, different regard for human rights and different view of competition, and one that has put in place policies and programs that undermine the very values we hold dear: a fair and level playing field, transparency, reciprocity and market-driven competition.ⁱⁱⁱ

Threats to the DOE Complex: The Importance of S&T

Emerging technologies are increasingly at the center of global competition, providing the foundational research and developments that underpin future industries and drive economic growth. These emerging technologies will alter economic, political and security dynamics and directly affect national security and competitiveness. However, knowledge-based industries rely on collaborations and sharing of data, research and human capital across national borders. While this has always been a U.S. strength, it creates vulnerabilities in our innovation base as some countries use these collaborations and exchanges to support the expropriation of existing know-how and talent. This often includes the acquisition of technology and technological know-how through legal, illegal and extralegal means.

Losing our technological edge and the influence it entails will have far-reaching implications beyond scientific disciplines. Increasingly this is also not about military technologies, but dual-use technologies and commercial applications. Future strength will be built on 5G, AI, biotechnology, new materials and areas currently researched in our national labs. While DOE may still be best known for stewarding our nuclear deterrent, it also is described as catalyzing the transformative growth of basic and applied scientific research and the discovery and development of new clean energy technologies. It prioritizes scientific innovation as a

cornerstone of U.S. economic prosperity—and in my opinion is an under-appreciated resource that incorporates the lifecycle of tech development.¹ Through its labs and plants, the government builds a technically capable workforce that will support future discovery and industry.

Additionally—and importantly—DOE’s work is also a window into the priorities of the U.S. government.

The Threat from China:

While China is not the only country that targets U.S. technology and the DOE complex, according to the ODNI’s 2023 Annual Threat Assessment² “China is the top threat to U.S. technological competitiveness, as it targets key sectors and proprietary commercial and military technology from the U.S. and allied companies and institutions.” This puts the DOE complex directly in China’s crosshairs given the depth, breadth and importance of its mission.

Beijing views technology—and the robust S&T infrastructure needed to develop it—as a national asset. The way it has structured its system to reach this goal is inherently at odds with key assumptions of the global norms of science which are built on transparency, reciprocity and sharing. Beijing, especially Xi, looks at development as a zero sum game and that government support for key industries—the emerging technologies^[1] such as AI, next generation communications and biotechnology—gives China an advantage. Xi’s statements include the following:

- “We must regard science and technology as our primary productive force, talent as our primary resource, and innovation as our primary driver of growth,” (November 2022)
- “We should seize the commanding heights of technological innovation.” (May 2018)
- “Artificial Intelligence is a vital driving force for a new round of technological revolution and industrial transformation. China must control artificial intelligence and ensure it is securely kept in our own hands” (October 2018).^[2]
- In a May 30, 2016 speech at the National S&T Innovation Conference to CAS, CAE, and CAST, Xi Jinping stated that “science and technology is a national weapon” and that “if China wants to be strong... it must have powerful science and technology.”^[3]
- “In today’s world, S&T innovation has become a critical support for increasing comprehensive national strength... whoever holds the key to S&T innovation makes an offensive move in the chess game of S&T innovation and will be able to preempt the rivals and win the advantages.” (June 2014)

Drivers of Technology Acquisition: Central Government S&T PLANS

¹ <https://www.energy.gov/science-innovation>

² <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>

China recognizes that future strength will be built on 5G, AI, biotechnology and advanced manufacturing. Its S&T development plans focus its efforts on acquiring technology that will help build these future industries, as well as the supporting industries that enable them. These are not always the “cutting edge” technology, but they either fill a strategic gap or help China control key supply chains for materials or goods.^{iv} China’s priorities are laid out in major policies like the Medium- and Long-Term Development Plan (MLP), Strategic Emerging Industries Strategy, and Made in China 2025.^{[1][2][3][4]} In pursuing these technologies, China’s lack of transparency with collaborators and aggressive technology acquisition practices pose increasing national security concerns. The policies focus not only on specific technology areas but seek to create the environment to foster innovation and development, and most importantly build a national innovation base that will be the foundation for future economic growth and military modernization that Beijing controls. Below is a selection of these plans and policies: ^[5]

The Medium and Long Term Plan for S&T Development, 2006-2020 ([中长期科技发展规划, 2006-2020](#)) lays out a development strategy that is reliant on returnees, foreign collaboration, and adds a new dynamic of using the R&D laboratories of international companies that have flocked to China as another medium through which it can acquire the skills needed for China to move forward. ^v The MLP, has 16 “mega-projects” that include:

- Core electronic components;
- High-end generic chips, and basic software;
- Extra large-scale integrated circuit manufacturing and technique;
- New-generation broadband wireless mobile telecommunications;
- Advanced numeric-controlled machinery and basic manufacturing technology;
- Large-scale oil and gas exploration;
- Large advanced nuclear reactors;
- Water pollution control and treatment;
- Genetically modified new-organism variety breeding;
- Drug innovation and development;
- Control and treatment of AIDS, hepatitis, and other major diseases;
- Large aircraft;
- High-definition Earth observation systems; and
- Manned aerospace and Moon exploration.

There are three “mega-projects” that have not been publicly disclosed but are most likely:

- the Beidou satellite project;
- the high-energy laser project; and
- hypersonic vehicle.

China’s plans for Strategic Emerging Industries^{vi} also lays a blueprint for its future goals of dominating key sectors. It articulates how its goals are securing the China market first on the way to building global champions, creating a model for how China breaks into and controls key sectors. China considers the following its strategic emerging industries:

- energy efficient and environmental technologies;
- next generation information technology;
- biotechnology;
- high-end equipment manufacturing;
- new energy (such as solar or wind);
- new materials; and
- new energy vehicles.

Two studies produced by Georgetown University's Center for Security and Emerging Technology (CSET) provide additional details about the type of technologies China is seeking. The first uncovers how China uses S&T diplomats in embassies around the world to find and broker deals for a wide range of technology from AI and biotechnology, to items needed in factories such as vacuum seals and materials. China's "S&T Diplomats" (科技外交官), broker transfer deals and coordinate with overseas experts to fulfill technology wish lists for Chinese entities. More than half of the 642 projects examined were biotechnology or AI projects.^{vii} The second study looks at what China describes as "strangle-hold" technologies^{viii}—or things where China has a gap. This list includes items such as different kinds of metrology, heavy duty gas turbines and materials for aircraft development, as well as the importance of quality in these areas. This relates to technological know-how which is equally important and why talent and training is targeted and sought after.

The "13th Five-year Plan for Military and Civil Fusion"^[i] was established in 2017 and focused on emerging technologies. The plan specifically calls for a "cross-pollination of military and civilian technology in areas not traditionally seen as 'national security issues,' such as quantum telecommunication and computing, neuroscience and brain-inspired research," and states that such projects will be supported by foreign outreach initiatives. In addition to these overarching projects, there are programs to develop specific high-tech areas such as biotechnology,^[ii] integrated circuits,^[iii] and "next-generation" artificial intelligence.^[iv] Each such program highlights the role foreign "talent" is expected to play.

China's legal system also complicates collaborations and the DOE complex's interactions with scientists and students from China. Many of China's laws compel its citizens to support its strategic goals—meaning visitors from China have to share information and data with Chinese entities if asked regardless of the restrictions placed on that data.^{ix} These are China's central government laws and include:

1. National Security Law (2015).^x
 - Article 77: Citizens and organizations shall perform the following obligations for safeguarding the national security: Provide national security authorities, public security authorities and military authorities with needed support and assistance.
2. Counterterrorism Law (2015).
 - Article 9: All work units and individuals are obligated to aid and assist the relevant departments in carrying out of counterterrorism work. If suspected terrorist activities or suspected terrorists are discovered

3. Cyber Security Law (2016).^{xi}
 - Article 28: Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.
4. National Intelligence Law (2017).
 - Article 7: All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with the law, and shall protect national work secrets they are aware of.

Human Cost of China's Behavior: The Role of Non-Traditional Collectors

One of the biggest challenges to understanding the scale and scope of China's actions, and designing mitigation strategies is China's use of what are called "non-traditional collectors." These are the experts—scientists, students and business people—who work on particular research projects in different industries and target technology and technological information. This is a different methodology and is documented in Chinese language policy documents over the last several decades.^{xii} Our system—and I would add our institutions and the authorities we have granted them—is not designed to counter this kind of threat. Traditionally, counterintelligence has focused on intelligence officers, military end-use and illegal activities. I tell you today, if we only focus on trying to mitigate China's illegal actions, those undertaken by intelligence officers or those only related to military technology, we will fail.

The Chinese government's explicit efforts to exploit its diaspora—and our innovation base—must be addressed and countered. China's exploitation of its diaspora is also a threat to the great majority of persons of Chinese ethnicity who play no part in this, but are tarnished and may be subject to unjustified criticism because of China's actions. This makes for a difficult balance. Our response must be two-handed—protect the rights of the people targeted by the Chinese Communist Party (CCP) while dealing with transgressions. Notable here is the fact that increasingly, the CCP targets non-ethnic Chinese³ scholars and scientists too, showing how this issue is not, in essence, one of ethnicity. Thus, the United States must continue to encourage academic exchange and an influx of scientific talent while at the same time find nuanced policy solutions, not only to stop the hemorrhaging of critical military and industrial technologies, but also, crucially, to play offense and continue to grow our national innovation base. This is also true for U.S. allies and like-minded countries worldwide.

The human cost of China's policies accrues in both directions, as Beijing disadvantages and tarnishes its own scientists who are trying honestly to work within global norms, because its domestic laws compel the disclosure of data/information. In this sense, the U.S. and other western countries are also culpable. By treating China as a neutral actor, and pretending that we operate within the same kind of system, we undercut those scientists and institutions in China trying to follow international norms. By not holding the Chinese government accountable, we give credence to a system that deprives China's educated elite from the dignity they aspire to and deserve. The Chinese people deserve better.

Talent Programs^{xiii}

The CCP and Chinese government continue to view Western education—and the DOE complex—as an entry point into the U.S. innovation base because it is an easier target. Xi has called human capital the "first resource"^{xiv} and China's policies reflect this.

³ While most of China's talent programs are focused on individuals that are ethnically Chinese regardless of citizenship, China increasingly targets others as well.

- Chinese government's National Medium and Long-term Talent Development Plan (2010–2020), stated that talent was core to the country's social and economic development and set detailed national talent targets.^{xv}
- 2017: "Plan to Build a National Technology Transfer System." A comprehensive articulation of China's tech transfer system. The acquisition of "high-level overseas talent"—both ethnic Chinese scientists from abroad and other foreign scientists—is emphasized throughout.
- 2016: "Planning Guide for Manufacturing Talent Development." Joint plan to import (another) "1000" foreign experts able to make "breakthrough" improvements, via talent programs and other venues. Emphasizes recruiting from "famous overseas companies."
- CAST's "HOME Program" (or Haizhi Plan, 海智计划),^{xvi} instituted in 2004 by the Chinese Association for Science and Technology to "Help Our Motherland through Elite Intellectual Resources from Overseas," and supported by China's central and local governments. Its 2019 slate includes 29 projects.^{xvi}

In addition to these overarching projects, as mentioned previously there are programs to develop specific high-tech areas such as biotechnology, integrated circuits, and "next-generation" artificial intelligence. Each such program highlights the role foreign "talent" is expected to play.^{xvii}

China's strategy to target the DOE lab complex, and U.S. technology in general is coordinated, massive, and comprehensive. It has a multifaceted effort to acquire technology and technological know-how using legal, illegal and extralegal approaches to fill its strategic gaps.^{xviii} Below is a more complete list of methodologies China uses to target technology and are seen throughout the DOE complex:

"Legal Transfers"⁴

- China-based subsidiaries of foreign companies
- Competitions (companies, universities)
- Conferences and colloquia
- Direct technology purchases
- Enrollments at foreign universities with ties to DOE
- Investments / acquisition of companies

Illegal Transfers

- Breach of contract
- Computer network exploitation
- Copyright infringement
- Reverse engineering with technological knowledge gained from the DOE complex

Extralegal Transfers

- China-based overseas returnee facilities
- Chinese professional associations
- Technology transfer forums

⁴ China often uses legitimate forums and collaborations as an entrée point to work in the "grey" area and target technology and technological know-how.

- Chinese student and scholar associations
- University-linked “innovation” parks
- Technology consulting companies

China has an extensive bureaucracy—both in China and throughout the world—set up to support its technology acquisition activities. Many of these organizations seem benign at first, but they are arms of the state and represent a very different system than the U.S. and other collaborators. Below is an overview of some of this bureaucracy:

Central Government Offices

China’s technology acquisition efforts are supported by government offices, with central government management replicated at the local level. They include: The State Administration of Foreign Experts Affairs (SAFEA, 国家外国专家局),^{xxix} the Overseas Chinese Affairs Office (OCAO, 国务院侨务办公室), the Ministry of Human Resources and Social Security (MHRSS, 人力资源和社会保障部),^{xxx} Ministry of Science and Technology (MOST, 科学技术部), Ministry of Education (MOE, 教育部), the Chinese Academy of Sciences (CAS, 中国科学院),^{xxxi} and China’s clandestine services.^{xxii}

“Unofficial Bureaucracy”

China uses NGOs and front organizations that parallel official bureaucracy to support programs while offering plausible deniability to foreign participants. The China Association for Science and Technology (中国科学技术协会)^{xxiii} runs a “Help Our Motherland through Elite Intellectual Resources from Overseas.”^{xxiv} China’s United Front Work Department (统一战线工作部) and Western Returned Scholars Association (欧美同学会) support transfers in multiple ways.^{xxv} Other NGOs share staff and offices with their government counterparts, such as the China Overseas Exchange Association (中国海外交流学会), which fronts for OCAO, and SAFEA’s “China International Talent Exchange Association” (中国国际人才交流协会)^{xxvi} with multiple branches overseas.

Open source exploitation

China has operated a science and technology intelligence (STI) program since 1958 to identify useful technologies and facilitate their transfer, and seeks DOE information and data to support its strategic programs. Insiders put the number of workers at 100,000,^{xxvii} up from 60,000 in 1985.^{xxviii} Its budget can exceed state expenditure on R&D.^{xxix} These figures are matched by a level of professionalization among “STI workers” (科技情报工作人员) unrivaled elsewhere.^{xxx} Its accomplishments, heralded in book-length accounts, include support for nuclear weapons, missile, and satellite programs.^{xxxi}

Overseas Advocacy Groups

Some 200 ethnic Chinese professional associations abroad accumulate the science, engineering, and enabling skills sought by China.^{xxxii} Many of these groups were created independently by expatriates while others were launched at the PRC’s behest. Some 61 percent “exchange

technical information, bring scientists to China, or contribute to specific Chinese talent plans.”^{xxxiii} Half advertise their support for China on the Chinese language versions of their websites only,^{xxxiv} and many acknowledge their raison d’être as “serving China” (为国服务).

Technology Parks

Ranging from modest offices to multi-acre, multi-story mega-centers, China has put in place Technology Transfer Centers, or Overseas Chinese Scholar Pioneering Parks, National Innovation Centers for New and High Technology, etc.,^{xxxv} that are subsidized clearinghouses for to transfer foreign IP to China. Studies done in 2010,^{xxxvi} 2016,^{xxxvii} and 2019^{xxxviii} traced their growth from fewer than 300 to its present number of some 2,000 facilities.

Additionally, exploitation of Chinese language sources uncovered two-dozen major “notifications” by the State Council, Communist Party Central Committee, and national ministries between 1994 and 2020 to facilitate access to foreign technology “by various means” (以多种方式).^{xxxix} Included are subsidies for “short term” returnees and “dual base” operations, where research abroad is mirrored in China; indigenization enclaves; “talent” programs; and incentives to transfer “patents, scientific research results, or proprietary technology.”^{xl} The directives are backed by measures from local authorities and these groups actively reach out to scientists currently in the DOE complex.



Figure 1: Above is a graphic representation of China's S&T development and technology transfer efforts. China takes a holistic approach to developing its S&T infrastructure and employs all facets of its government and society to acquire technology.

Conclusions

China's holistic approach to development, blurring what is civilian, what is military, what is private and what is public—has deep implications for the DOE complex. It impacts the basis for entry of Chinese students and post-docs into U.S. labs because of China's ability to compel citizens to share information. It also challenges existing export and visa policies that build their restrictions around affiliations with a military end-users but make exceptions for civilian uses. To the Chinese leadership, every civilian use is also a potential military use.

China's policies to target the DOE complex are the expression of a deliberate, state-sponsored strategy to save time and money, and "leap-frog" to the international forefront by leveraging the advances of other nations. While military and intelligence related technology are still targeted, China's efforts increasingly focus on technologies of the future such as AI, biotechnology and precision medicine and advanced manufacturing and materials.^{xli}

There is no magic bullet to solving these complex challenges but, mitigation strategies should include investments in our own future, as well as concrete steps in the short-term that focus on protecting our innovation base. These steps should include stemming China's influence in our academic and research institutions through enhanced reporting requirements for resources from the Chinese government and talent programs or dual appointments, and tying collaborations and access to U.S. facilities and data to meeting the agreed upon criteria of any S&T agreement. Finally, the U.S. needs a long-term strategy to deal with a nation state with a very different system. To date, our attempts at exquisite rules-based, laws-based mitigation efforts that try to carve out collaborations with "civilian and private" entities fall flat. Below are additional suggestions for what a mitigation strategy should include:

Improve ourselves: The United States and other liberal democracies must invest in their respective futures. Not all discovery has immediate commercial applications—it took 30 years from discovery to development of the Lithium-ion battery. We must accept that everything should not be only about the lowest cost, but instead focus on the highest value for the nation. We must build research security into future funding programs. What has been laid out here demonstrates the depth and breadth of China's efforts to target our technology, and the lengths it will go to acquire it. The United States must encourage STEM education and create support networks for under-represented populations in the STEM fields. Many students leave STEM fields in the first year. If students are working their way through college, they may not have time for lab work or research experiences. Funding should be provided for this, as we are leaving whole segments of our population behind.

Face the facts: Beijing doesn't play by free-market rules, it does not respect intellectual property, it is willing to act directly or indirectly to ensure its favored companies win in the market, and it doesn't share the same views on political openness the United States, Europe and other "like-minded" countries have long shared. Engagement with China has not made it more open, and it has not acquiesced to existing norms and rules. Acknowledging this reality complicates mitigations, because we are not negotiating on individual policies but against a different system. Moreover, the people who come here, however well-meaning they are personally, are to a greater or lesser extent beholden to China's system.

Increase Transparency: Existing policies and laws are insufficient to address the level of influence the Chinese Communist Party exerts in our society—especially in academia. The CCP exploits identity politics through United Front influence campaigns and other state efforts. This must be addressed and made public. The recent revelations about influence in Facebook are a start. By the same token, we must increase reporting requirements for foreign money at our academic and research institutes, as well as state and local governments to better identify these avenues of influence. Talent programs set up by the Chinese government, because of the restrictions and rules they place on the participants, present a conflict of commitment where

participants are often serving two different organizations, which at best introduces conflicts of interest and in some cases fraud, and other illegal activity. Universities, government labs and research institutions should have clear reporting requirements and rules on participation. Recent actions by DOE and some academic institutions are a good first step but still don't address the entirety of the problem.

Ensure True Reciprocity: Too often S&T agreements between U.S. and China's entities do not result in true reciprocity including sharing of data from the China, access to China's most advanced institutions, and interactions with China's scientists without government interference. Connecting China's reciprocity and sharing of scientific data to its access to U.S. institutions and big science facilities is a leverage point. For too long we have looked the other way when China has not followed through on the details of the agreements that it has entered into. American taxpayers should receive benefit from the research they are supporting.

Bolster Cooperation and Alliances: Greater cooperation and integration with Allies and like-minded countries will not only foster the development of emerging tech industries, but also create alternative innovation hubs that mitigate China's unfair practices and continue to foster the global norms of science.

In moving forward, I leave the committee with the following thoughts:

- Extreme propositions, such as closing our eyes (*laissez faire*) or closing our doors, only benefit China—the latter by discrediting en masse all efforts to address the problem and by depriving ourselves of the contributions of foreign-born scientists.
- China's policies and plans form a complementary web of development and industrial policies for emerging technologies—and talent growth—and most importantly build a national innovation base that will be the foundation for future economic growth and military modernization that Beijing controls. *It is not where they are today in certain fields, but the rate of change that we should focus on.*
- China's policies are increasingly challenging for the United States and its allies to counter with policy measures because *most policy measures are tactical and not designed to counter an entire system that is structurally different.*

What will also make this difficult is that the reality that China is presenting is inconvenient to those benefiting in the short-term. This includes companies looking for short-term profits, not long-term sustainability of a particular industry, academics that benefit personally from funding or cheap labor in their labs, and former government officials who cash in as lobbyists for China's state-owned and state-supported companies. China is masterful at divide-and-conquer, identity politics, controlling the narrative and falsely presenting engagements as "win-win." In reality, China wins twice—both by gaining technology and controlling the narrative in such a way that its behavior, over time, gains legitimacy.

¹ Ibid.

² William C. Hannas and Didi Kirsten Tatlow, *Beyond Espionage: China's Quest for Foreign Technology* (Routledge 1st edition, September 2020); Alex Joske, "Hunting the Phoenix," Australian Strategic Policy Institute, 2020, <https://www.aspi.org.au/report/hunting-phoenix/>; Receipts of local UFWD paying overseas scientists available at: "The distribution list of provincial-level projects for the introduction of foreign intelligence special funds at the provincial level in 2018" [2018 年省级引进国外专利专项经费直项目分配明细表], <http://web.archive.org/web/20201112190122/http://webcache.googleusercontent.com/search?q=cache:33AKAaZ3lPcE4oP33Arklnan.gov.cn%2Frs%2Fcxq%2Fzge%2F201802%2F9516964%2Ffiles%2F1e4d51ddn4f9b706ad5a90490.xls&cd=3&hl=en&ct=cr&url=en>

³ E.g., "The IP Commission Report," The Commission on the Theft of American Intellectual Property (May 2013). Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*, (Routledge, 2013) hereafter "CIE." Michael Brown and Paveet Singh, "China's Technology Transfer Strategy" (DILUX, February 2017). Section 301 *Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Office of the United States Trade Representative (27 March 2018). U.S.-China Economic and Security Review Commission, "2019 Annual Report to Congress" (November 2019).

⁴ "十三五" 科技军民融合发展专项规划. MOST, CMC, 2017; 国务院关于印发"十三五"国家战略性新兴产业发展规划的通知. State Council, 2016; 国家科技创新基地优化整合方案. MOST, MOF, National Development and Reform Commission, 2017; "十三五" 科技军民融合发展专项规划. MOST, CMC, 2017; Simon and CAO, "China's Emerging Technological Edge: Assessing the Role of High-End Talent". Cambridge University Press, 2009.

⁵ Cao et al., *China's 15-year science and technology plan*, Physics Today, December 2006; McGregor, James, China's Drive for "indigenous Innovation" A Web of Industrial Policies, Global Regulatory Cooperation Project, US Chamber of Commerce.

⁶ XU, Yingying, "The Strategic Emerging Industries: A new stage for Manufacturing in China" The Economist, 13 March 12; www.most.gov.cn/en/programmes/200610120061009_36225.htm; www.863.gov.cn/; Osnos, Evren, Green Giant: Beijing's Crash program for clean Energy, The New Yorker, 21 December 2009; www.gov.cn/english/2006-02/09/content_184156.htm; Du Minghua, "863" Hi-Tech Program Blueprinting China's Future, 1 January, 200, from China Education and Research network website: www.edu.cn/achievement_150920060323/20060323_4403.shtml; Chinese government policy documents at: www.china.org.cn/english/scitech/34446.htm and Cao et al., *China's 15-year science and technology plan*, Physics Today, December 2006; "New Policies to be Issued to Lure Overseas Students Home," *People's Daily*, 29 July 2000, "China Allotted 200 Million Yuan for Students Returned from Overseas," *People's Daily*, 22 January 2002; McGregor, James, China's Drive for "indigenous Innovation" A Web of Industrial Policies, Global Regulatory Cooperation Project, US Chamber of Commerce.

⁷ Ryan Fedasick, Emily Weinstein, and Anna Puglisi, "China's Foreign Technology Wish List," Georgetown University, Center for Security and Emerging Technology, May 2021.

⁸ PRC Ministry of Education (教育部) website, September 24, 2020. This article is a summary of a series of 35 separate articles that Science and Technology Daily (科技日报)—a weekday newspaper published under the auspices of (代管) the PRC Ministry of Science and Technology (MOST; 科技部)—published in 2018.

⁹ Findings of the Investigations into China's Acts, Policies and Practices related to Technology Transfer, Intellectual Property and Innovation under Section 301 of the Trade Act of 1974", March 22, 2018, USTR.

¹⁰ China's National Security Law (2015), Counterterrorism Law (2015), Cybersecurity Law (2016) and National Intelligence Law (2017).

¹¹ China's National Security Law (2015), Counterterrorism Law (2015), Cybersecurity Law (2016) and National Intelligence Law (2017).

¹² These policies include "two bases formula", "short-term visits" and "serve in place. See Hannas et al., Routledge 2013 more a more in depth treatment of these policies.

¹³ Original CSET Data Visualization, "Chinese Talent Program Tracker," Center for Security and Emerging Technology, November 2020. <https://doi.org/10.51593/20200066>

- ^{xiv} “十三五”生物技术创新专项规划 (*13th Five-year Plan for Biotechnology Innovation*). MOST, 2017; 国家集成电路产业发展推进纲要 (National Integrated Circuit Industry Development Plan). State Council, 2014; 新一代人工智能发展规划. (Next-Generation Artificial Intelligence Development Plan). State Council, 2017; “Why is Xi Jinping’s ‘First Resource’ so important?” [“习近平眼里的‘第一资源’为何如此重要”], *People* [人民网], July 18, 2018, <http://politics.people.com.cn/n1/2018/0718/c1001-30155931.html>; 国家技术转移体系建设方案. State Council, 2017; 制造业人才发展规划指南. MOE, MHRSS, MIIT, 2016.
- ^{xv} “十三五”科技军民融合发展专项规划. MOST, CMC, 2017.
- ^{xvi} Hannas and Tatlow, “China’s Quest for Foreign Technology: Beyond Espionage” Routledge, 2020.
- ^{xvii} “十三五”科技军民融合发展专项规划. MOST, CMC, 2017; “十三五”生物技术创新专项规划 (*13th Five-year Plan for Biotechnology Innovation*). MOST, 2017; 国家集成电路产业发展推进纲要 (National Integrated Circuit Industry Development Plan). State Council, 2014; 新一代人工智能发展规划. (Next-Generation Artificial Intelligence Development Plan). State Council, 2017.
- ^{xviii} Cory Bennett and Bryan Bender, How China Acquires “The Crown Jewels” of US technology, POLITICO, May 22, 2018; <http://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413>; Jackie Northam, China Makes Big Play in Silicon Valley, NPR, Oct. 7, 2018.
- ^{xix} Formerly independent but now part of MOST.
- ^{xx} Formerly China’s Ministry of Personnel.
- ^{xxi} CAS’s status as an appendage of the PRC government was confirmed by a senior staff member in a letter to the editor of *Nature* magazine on October 20, 2019, www.nature.com/articles/d41586-019-03205-z.
- ^{xxii} Matthew Brazil and Peter Mattis, *Chinese Communist Espionage: and Intelligence Primer*, Naval Institute Press, 2019.
- ^{xxiii} CAST’s formal affiliation with the PRC government is demonstrated in Hannas, Mulvenon, Puglisi, 2013, p. 97.
- ^{xxiv} Hannas and Chang, “Chinese Technology Transfer—Introduction,” in Hannas and Tatlow, eds., 2021, pp. 11-12.
- ^{xxv} Alex Joske and Jeffrey Stoff, “The United Front and Technology Transfer,” in *Ibid.*, pp. 258-274. Ryan Fedasiuk, “Putting Money in the Party’s Mouth: How China Mobilizes Funding for United Front Work,” *The Jamestown Foundation*, September 16, 2020.
- ^{xxvi} Formerly the “China Association for the International Exchange of Personnel” (CAIEP).
- ^{xxvii} Zeng Jianxun (曾建勋), “基于国家科技管理平台的科技情报事业发展思考 (Reflections on the Development of the Scientific and Technical Information Industry Based on the National Science and Technology Management Platform),” *情报学报 (Journal of the China Society for Scientific and Technical Information)*, 2019: 38 (3), pp. 227-238.
- ^{xxviii} Miao Qihao, “Technological and Industrial Intelligence in China: Development, Transition and Perspectives,” Prescott and Gibbons, eds., *Global Perspectives on Competitive Intelligence*, Alexandria, VA: Society of Competitive Intelligence Professionals, 1993, pp. 49-53.
- ^{xxix} Chen Jiugeng, “Actual Strength of S&T Information Service System in China,” *China Information Review*, 2006: 10, pp. 17-22.
- ^{xxx} Hannas and Chang, January 2021.
- ^{xxxi} Huo Zhongwen (霍忠文) and Wang Zongxiao (王宗孝), *国防科技情报源及获取技术 (Sources and Methods of Obtaining National Defense Science and Technology Intelligence)*, Beijing: Kexue Jishu Wenxuan Publishing Company, 1991, and 中国科学技术信息研究所 (ISTIC), 甲子辉煌—中国科学技术信息研究所成立60周年纪念 (*60 Years of Glory—The 60th Anniversary of the Founding of the Institute of Science and Technical Information of China*), Beijing, 2016.
- ^{xxxii} Hannas, Mulvenon and Puglisi, 2013. Ryan Fedasiuk and Emily Weinstein, July 2020.
- ^{xxxiii} Fedasiuk and Weinstein, July 2020.
- ^{xxxiv} *Ibid.*
- ^{xxxv} Hannas, Mulvenon, Puglisi, 2013, p. 176.
- ^{xxxvi} *Ibid.*
- ^{xxxvii} Ryan Fedasiuk, Georgetown University, unpublished CSET research.
- ^{xxxix} Hannas and Tatlow, eds., 2021, especially pp. 9-11.
- ^{xl} *Ibid.*, p. 10.
- ^{xli} Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*. (Routledge, 2013) hereafter “CIE.” E.g., “The IP Commission Report.” The Commission on the Theft of American Intellectual Property (May 2013). Michael Brown and Pavneet Singh, “China’s Technology Transfer Strategy” (DIUX, February 2017). Section 301 *Report into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Office of the United States Trade Representative (27 March 2018). U.S.-China Economic and Security Review Commission, “2019 Annual Report to Congress” (November 2019).

The CHAIRMAN. Thank you.
And now we will have Mr. Wheeler.

**STATEMENT OF ANDREW WHEELER, FELLOW AND VICE
PRESIDENT, HEWLETT PACKARD LABS AND HPC AND AI AD-
VANCED DEVELOPMENT, HEWLETT PACKARD ENTERPRISE**

Mr. WHEELER. Chairman Manchin, Ranking Member Barrasso, and distinguished members of the Committee, thank you for the opportunity to testify today and thank you for this Committee's support for the Exascale Computing Initiative. My name is Andrew Wheeler and I lead advanced development in high performance computing and artificial intelligence and serve as the Director of Hewlett Packard Labs, the central applied research group for Hewlett Packard Enterprise. While we trace our roots back to the original Hewlett-Packard Company, as many of you know, Hewlett Packard Enterprise was formed as a new publicly traded company in November 2015. At HPE, we fundamentally believe that AI will have as significant an impact on our lives as any technology to date. Training the largest AI models is a supercomputing problem, and at HPE, we build the world's best supercomputers. With our partners at the Department of Energy, we co-design and co-build supercomputers that target complex scientific, engineering, and data-intensive workloads. These include systems at Sandia and Los Alamos National Laboratories in New Mexico, the National Renewable Energy Laboratory in Colorado, and the National Energy Technology Laboratory in Morgantown, West Virginia.

Our national investments in supercomputing have far-reaching benefits across the Federal Government. For example, our innovations in computing power and density that we provide to the DOE are also being used across the Department of Defense, in the intelligence community, at the National Oceanic and Atmospheric Administration to forecast weather, and at the National Science Foundation centers. In fact, during the early stages of the COVID-19 outbreak, the national labs, including Argonne and Lawrence Livermore, used their supercomputers to accelerate a path to treatment to combat the disease. Using detailed digital simulations to analyze a vast set of drug candidates, researchers at Lawrence Livermore narrowed down the number of potential antibody candidates from an initial set of 100 duodecillion—that is a one with 40 zeros after it—to just 20. The lab's researchers accomplished this in weeks compared to the years it would take using other approaches.

In 2016, HPE was proud to be chosen as a key partner in the DOE's Exascale Computing Initiative, which was designed to accelerate the research, development, acquisition, and deployment of new technologies to deliver exascale computing and to usher in a new era of supercomputing speed and capabilities. Then, in May 2022, HPE, as part of a public-private partnership with Oak Ridge, achieved exascale computing with a computer that is more powerful than the world's next four fastest systems combined. To put exascale into context, the human brain can perform about one simple mathematical operation per second. An exascale computer can do at least one quintillion, which is one billion times a billion calculations in the same amount of time. The success of the Exascale

Computing Initiative restored the U.S. position as having the world's most powerful computer and also marked the creation of the world's largest AI system, which will soon be joined by systems installed at Argonne and Lawrence Livermore. The Exascale Computing Initiative was the model of success. Congress made the right investments. Our national labs challenged America's technology industry, and at HPE, we rose to the challenge.

In conclusion, while the United States has regained its rightful role as the world leader in supercomputing, now is not the time to rest on our laurels. The DOE national labs are producing results that researchers could only have dreamed of just a few years ago. Continued investment in this successful partnership is in our national, economic, and security interests, and HP looks forward to working with the U.S. Government to continue our global leadership.

[The prepared statement of Mr. Wheeler follows:]



**Hewlett Packard
Enterprise**

**Statement of Andrew Wheeler, HPE Fellow, Vice President and Director of
Hewlett Packard Labs at Hewlett Packard Enterprise before the Senate
Committee on Energy and Natural Resources**

**Hearing to examine recent advances in artificial intelligence and the
Department of Energy's role in ensuring United States competitiveness and
security in emerging technologies**

September 7, 2023

Chairman Manchin, Ranking Member Barrasso, and distinguished members of the committee, thank you for the opportunity to testify today. It is an honor to be here to discuss the importance of recent advances in artificial intelligence and the Department of Energy's mission to strengthen national security and competitiveness through cutting-edge technologies.

My name is Andrew Wheeler and I am Vice President and Director of Hewlett Packard Labs, the central applied research group for Hewlett Packard Enterprise that was established in 1966 by the founding company, which is widely recognized as the birthplace of Silicon Valley. As many of you know, Hewlett Packard Enterprise was formed as a new publicly traded company in November 2015. We have a rich, decades-long history of co-developing leadership computing with the U.S. government.

My testimony will highlight the role of U.S. public-private partnerships in co-designing and co-developing the next-generation supercomputing systems that are vital to unlocking value from AI and maintaining leadership in this critical technology.

Hewlett Packard Enterprise partners closely with U.S. federal agencies on R&D projects. Our work has advanced and achieved state-of-the-art capabilities for a range of technologies, including areas that are critical to increasing performance, speed, security, and productivity for growing data-intensive applications, such as AI, and that are driving demand for more computing and network bandwidth resources. These technologies include high-speed networking, silicon design for advanced high-performance computing and supercomputing, and neuromorphic computing.

I am currently directing research and advanced development efforts for emerging technologies, including trustworthy AI, quantum computing, security, silicon photonics, and systems architecture, among other initiatives.

In addition to overseeing our Labs, I also lead our High-Performance Computing (HPC) and Artificial Intelligence (AI) Advanced Development and Chief Technology Office organizations to fuel future innovations that can be leveraged across our company. Our Labs team and the HPC & AI Advanced Development organization collaborate with the U.S. government and its national laboratories, academia, and industry partners to deliver innovation that propels our growth as a nation and as a society.

HPE's world-leading supercomputers support the nation's mission-critical initiatives

HPE's expertise is deeply rooted in computing. We design trusted systems from the ground up to deliver powerful technology. For decades, we have influenced the design and engineering of the world's leading semiconductor chips to deliver significant advancements in performance and capabilities for emerging applications.

We are the leading expert in supercomputing, delivering the world's most powerful systems. Bolstered by HPE's acquisition of Silicon Graphics and Cray, a pioneer in supercomputing, we provide world-leading supercomputers that continue to demonstrate significant value in accelerating scientific discovery and enabling new techniques in engineering.

For decades, HPE has worked closely with the Department of Energy to jointly design, develop, and engineer many world-first achievements in supercomputing. Most recently, together with the Department of Energy, HPE built the first U.S. exascale systems – “Frontier” at Oak Ridge, “Aurora” at Argonne, and “El Capitan” at Lawrence Livermore for the National Nuclear Security Administration (NNSA) to advance R&D for the nation's nuclear deterrent.

With our partners at the DoE, we co-design and co-build supercomputers that target complex scientific, engineering, and data-intensive workloads for U.S. national laboratories and R&D centers across the Department. These include Sandia and Los Alamos National Laboratories in New Mexico, National Renewable Energy Laboratory (NREL) in Colorado, and National Energy Technology Laboratory (NETL) in Morgantown, West Virginia.

The investments in supercomputing made by the DoE have far reaching benefits across the federal government. For example, the innovations in computing power and capabilities that we provide to the DOE are being used by the Department of Defense and the intelligence community, including the Stennis Space Center Mississippi for the U.S. Navy, MIT Lincoln Laboratory in Massachusetts, and the Army and Air Force labs to advance defense missions.

Our supercomputers are used to power the nation's weather forecasting, including predicting catastrophic events. The National Oceanic Atmospheric Administration (NOAA) has adopted our supercomputers in its labs and research centers in Phoenix, Arizona, Virginia, and Fairmont, West Virginia.

HPE-built supercomputers can be found in labs and research centers sponsored by the National Science Foundation, such as the National Center for Atmospheric Research (NCAR) in Wyoming, the National Center for Supercomputing Applications (NCSA) in Illinois, Stony Brook University in New York, and the Pittsburgh Supercomputing Center in Pennsylvania.

Using supercomputing to increase U.S. industry competitiveness with faster time-to-market innovation

Additionally, supercomputers are impactful to R&D and product design across the commercial sector, contributing to our nation's competitiveness. HPE works closely with leading U.S. companies in advanced manufacturing, energy, aerospace, transportation, health care, automotive, and pharmaceuticals to deliver advanced supercomputing to accelerate U.S. innovation in the market.

According to a study by Hyperion Research, an industry analyst firm that examines the high-performance computing and supercomputing industry, supercomputers have contributed to product innovation, such as automotive, aircraft, and pharmaceuticals, that are valued at more than \$100

trillion over the last 25 years. Hyperion also estimates that the economic value created by applications running on supercomputers has exceeded \$3 trillion over the past 25 years.

Hyperion conducted a study on 175 industrial firms and found that on average, companies realized \$452 for every \$1 they invested in HPC and estimated that 175 HPC-supported projects created 2,335 new jobs.

Realizing transformative benefits of AI with supercomputing

At HPE, we fundamentally believe that AI will usher in a new wave of productivity and have as significant an impact as the advent of mobile, cloud, and Web 2.0. AI will equip Americans with better tools to automate, analyze, and solve problems faster. Making breakthroughs in scientific research and development will strengthen our national security, increase our competitiveness, and help maintain American leadership.

Given the massive, specialized computing performance and scale that supercomputers deliver, these systems are ideally suited to efficiently train AI models and run AI applications. By applying artificial intelligence to research conducted on supercomputers, scientists and engineers can further their research and accelerate discoveries.

For example, during the early stages of the COVID-19 outbreak, the national labs, including Argonne and Lawrence Livermore, used their supercomputers to accelerate a path to treatment to combat the disease.

Researchers used AI on detailed, digital simulations of molecular interactions between the virus' spike protein and a vast data set of drug candidates. Researchers at Lawrence Livermore National Laboratory found this approach to be incredible – narrowing down the number of potential antibody candidates from an initial set of 100 duodecillion – that's a 1 with 40 zeros after it – to just 20. The lab's researchers also accomplished this in weeks, compared to the years it would take using other approaches.

The U.S. ushers in the fastest computing made possible today with exascale

In 2016, to maintain leadership in science and technology, and advance our nation's position in AI, the Department of Energy sought to break barriers in computing speed and usher in a new era of supercomputing by forming the Exascale Computing Initiative (ECI). The initiative was formed within the Department of Energy, as a partnership between two DOE organizations: the Office of Science (SC) and the National Nuclear Security Administration (NNSA).

HPE was proud to be a key partner for the ECI, which was designed to accelerate the research, development, acquisition, and deployment of new technologies to deliver exascale computing, and to usher in a new era of supercomputing speed and capabilities. The exascale threshold delivers up to 10X faster performance than most of the world's most powerful supercomputers and offers insights and the ability to solve complex problems that were previously impossible.

As part of the ECI, a program called PathForward was introduced that granted \$258 million across select U.S. technology companies, including HPE and Cray. The grants allowed us to design and build a completely new supercomputing architecture from the ground up that can scale to an unprecedented speed while consuming significantly lower power.

The resulting solution -- the HPE Cray EX supercomputer -- was selected as the supercomputing platform for U.S. exascale systems. The HPE Cray EX supercomputer is designed with end-to-end,

cutting-edge technologies spanning CPUs, GPUs, unique Ethernet capabilities that can scale to tens of thousands of GPUs, software, and sophisticated closed-loop liquid cooling capabilities.

Then in May 2022, HPE ushered in exascale computing with Frontier, which represents an increase of nearly 70,000-fold over the past 20 years. This was a pinnacle moment in supercomputing that restored the U.S. position as having the world's most powerful supercomputer. The massive achievement also demonstrated the essential role of public-private partnerships in advancing national technological priorities.

Since its debut last year, Frontier has already helped scientists make breakthroughs in aerospace, medicine, and nuclear physics. Frontier is also the world's largest AI system, bringing nearly 40,000 GPUs to task to build and train large-scale AI models, improve model accuracy, and accelerate outcomes. Those technologies are being adopted by other U.S. national laboratories and across federal agencies, including Los Alamos National Laboratory, National Oceanic Atmospheric Administration (NOAA), National Renewable Energy Laboratory (NREL), National Energy Research Scientific Center (NERSC) at Lawrence Berkeley Lab, and the National Center for Atmospheric Research (NCAR), the Department of Defense, National Aeronautics and Space Administration (NASA), National Institutes of Health (NIH), and the Department of Interior.

Realizing the full potential of AI with advancing computing

In a DOE-led published report, "[AI For Science](#)," the DOE details opportunities for applying new AI techniques to 16 application areas, including science, energy, security, facilities, and other areas, that when advanced with AI, have the potential to transform the department's research capabilities.

The report identifies six broadly applicable AI building blocks to target a range of use cases, including fusion energy, nuclear deterrence, bio assurance, advanced manufacturing, drug discovery, digital twin modeling for complex scientific domains, and personalized medicine.

To successfully execute these AI approaches and advance the DOE's national missions, we need to continue investing in advancing computing environments to support large-scale AI models.

AI model sizes have significantly grown over the years, requiring more computing resources. When training AI using a volume of complex data, it is critical that we provide the computing environment to do so efficiently if we want to realize the full potential of AI to solve problems.

With a higher requirement level of computing, requiring the capacity to run many GPUs, or accelerators, at once, commodity servers and the traditional public cloud are neither an efficient nor sufficient solution.

Building on exascale innovation to accelerate AI initiatives

By building on U.S. exascale leadership, the Department of Energy is exploring initiatives to leverage today's most powerful supercomputing technologies to support the DoE's AI mission and missions across disciplines throughout the federal government.

Just as it set out to build the world's most powerful supercomputer with exascale, the DoE aims to continue to build the world's most powerful AI systems and foundational models to target scientific research use cases across materials science, particle physics, molecular biology, chemistry, and environmental sciences.

We believe that this is an important initiative to accelerate our nation's mission of advancing AI at a larger scale and are working closely with the DOE and its national laboratories to enable this capability.

A recent study published by the National Academies, "[Charting a Path in a Shifting Technical and Geopolitical Landscape](#)," underscores the need for the DOE to achieve its goals. The study reinforces that exascale computing will allow the National Nuclear Security Administration (NNSA) to take full advantage of new computational approaches, but that we need to sustain investments in supercomputing if we want to continue to foster that innovation.

Continuing strong national investment in supercomputing to fuel AI and maintain leadership

In conclusion, while the United States has regained its rightful role as the world leader in supercomputing, now is not the time to rest on our laurels if we want to maintain that position. The DoE national labs are producing the types of results, harnessed from complex research, and speed of innovation that researchers could have only dreamed of just a few years ago. Continued investment in this success is in our national economic and security interests and HPE looks forward to working with the U.S. government to continue this legacy of global leadership.

The CHAIRMAN. Thank you.

Now, I will begin with our questioning. My first question will go to Secretary Turk and Dr. Stevens and Mr. Wheeler. In my testimony, I mention a study about how AI was used to provide clear and detailed steps to create a pandemic or bioweapon. The DOE and the labs are uniquely positioned to do extensive work in detecting and mitigating emerging technological threats related to an array of biotechnologies and nuclear security. So Mr. Turk and Dr. Stevens, what can the Department and the labs do to address these safety and security concerns?

Mr. TURK. Well, thanks for the question. You are right to raise this as an issue. The MIT study that you referenced and put into the record is one of those that is a real eye opener. It should be, especially for those who don't deal with these issues on a daily basis. So we have a real challenge here. As Professor Stevens and others have pointed out, AI can do a lot of good, but it can do a lot of harm here, right? It allows actors who are not as sophisticated scientifically or technologically to do certain things that could have huge, huge harm. So from the DOE side, I think we have some ability to be incredibly helpful working with others—Department of Defense, HHS, others as well. We have to remember that our national labs don't just work for the Department of Energy, they work for all the other agencies, and a lot of other agencies already have a lot of programs, including in the biodefense and biotech area.

We also, at the Department of Energy, know how to deal with classified information. We have our own intelligence branch. And that is incredibly important here as well. So we are not just relying on what is in the open record, but we have the best of what is going on from a scientific and certainly from an intel perspective.

The CHAIRMAN. Let me give you a quick overview of what I am trying to get to—I look back and we all remember when the internet was coming on board and it was born out of the labs. And then, by the 1990s—early 1990s—we had to do something. We created Section 230, thinking we would let it develop and be all it could be. We look back, and it's even more than what we thought it could be, and it has been used very effectively to help economies and help people all over the world. But it has been used very detrimentally too. So we are trying to not re-create that same environment here with AI. That is what we are looking at.

So what you saw, just with what the MIT students could do in one hour, it is alarming. And I have advised some of my colleagues about this. What can you do to stop something like that, and what kind of guardrails are needed?

Dr. Stevens, do you want to say something on that?

Mr. TURK. I was just going to say this is exactly why we need to invest in these capabilities, right? I mean, we need to be ahead of the curve.

The CHAIRMAN. Right.

Mr. TURK. And Professor Stevens can certainly get into that more.

Dr. STEVENS. Let me just try to outline quickly how we would approach that problem. So, of course, DOE is working with NIST on a thing called the AI Risk Management Framework, which is large-

ly currently envisioned as a process that uses humans to evaluate the trustworthiness and the alignment—that is, whether a model does something that you would like it to do or something that you don’t want it to do. I think the key thing here—there are actually two key problems that we have to solve. One is, we have to have the ability to assess the risks in current models at scale. There are over 100 large language models in circulation in China. There are more than a thousand in circulation in the U.S. A manual process for evaluating that is not going to scale. So we are going to have to build capabilities using the kind of supercomputers we have and even additional AI systems to assess other AI systems, and we can say this model is safe. It does not know how to build a pandemic or it won’t help students do something risky. That is one thing we have to do.

The second thing we have to do is, we have to understand the fundamental issue of alignment—what is called alignment—that is, building these models that align with human values and are reliable in aligning with human values. And that is a fundamental research task. It’s not something where we can just snap our fingers and say we know how to do it. We don’t know how to do it. Companies don’t know how to do it, labs don’t know how to do it, universities don’t know how to do it. That is one of the goals that we would have to have in a research program like this. So we need scale, the ability to assess and evaluate risk in current models and future models, and we need fundamental R&D on alignment and AI safety.

The CHAIRMAN. It’s growing so quickly and expanding—when we heard about it, and coming at it, you know, from our standpoint, to where we are today and to have a class study, and these were non-scientist students.

Dr. STEVENS. Yes.

The CHAIRMAN. To be able to get this. All right, how can we put that back—the cat back in the box?

Dr. STEVENS. I don’t think we can put it back in the box. I think we are going to be—we have to get smarter about how we manage the risks associated with advanced AI systems, and using the term that people are using quite a lot about being eyes-wide-open. There is no putting Pandora back in the box, right? Every person within the next few years is going to have a very powerful AI assistant in their pocket to do whatever it is that they can get that assistant to help them to do. Hopefully, most of that will be positive advances for society and so on. Some of that will be negative. We have to be able to understand how to reduce that negative element, detect it when it happens, and mitigate it either through laws or through other means—technical means.

The CHAIRMAN. Yes.

Dr. STEVENS. Before something dramatically bad happens. And I think that needs to be part of the technical agenda for the labs, and quite frankly, across the Federal Government.

The CHAIRMAN. I am going to take the liberty of having seven-minute rounds, so if you want to set that for seven minutes. Ms. Puglisi, did you want to speak on this at all? Do you have any comments?

Ms. PUGLISI. Sure. I think that is also important, as we look at AI as a tool of discovery, and in some ways you could say that the study that the classroom did was a discovery. There are a lot of steps though that need to happen from the time you go from a sequence into something that can really have a large-scale damage that is talked about. And since one of the things that we are actually taking a closer look at is—having the sequence is one thing, but then what are those follow-on steps? And so that is something that there is still a lot of—what chemistry, what biology has to go on in between that?

The CHAIRMAN. I guess in a nutshell, is it too late to put any guardrails on? Have we missed it?

Mr. WHEELER. Not entirely. I think there are many layers to this.

The CHAIRMAN. They are getting close.

Mr. WHEELER. I think there is both a policy aspect to this as well as, you know, kind of a research component. But as an example, on the policy side, like our own company, right, we spent over a year and a half developing what we call our AI ethics principles. And this is all about, you know, getting our thousands of engineers and users, you know, go through training around, okay, what does it mean to use AI in our product developments? You know, how are we going to deploy solutions that harness AI? And now, that can't solve every problem because, as you mentioned, there are bad actors that maybe wouldn't follow that same line of reasoning. And that's where I think the research investment comes into play. There is a broad field of study around this trustworthy AI, which ultimately can provide some of those guardrails you are asking about, but we are still really in the early days of some of that and deploying some of those solutions and there is a lot of work that is left.

The CHAIRMAN. Thank you.

Senator BARRASSO.

Senator BARRASSO. Thank you, Mr. Chairman.

Ms. Puglisi, just a couple things. You are an expert on Chinese science and technology policy. You very well outlined us in your opening statement the threats that China poses to government-funded research as well as private-sector development. So we have more than 4,000 Chinese nationals working in the Department of Energy labs. Are these employees vulnerable to the Chinese Communist Party—their talent recruitment programs? How does that work?

Ms. PUGLISI. Right, thank you.

The talent recruitment programs really do pose quite a challenge based on the principles that a lot of these individuals, when they sign these contracts, often obfuscate their participation. But I think, as I mentioned in my opening statement, it's really important as we go forward that we acknowledge the policies and programs that China has put in place and really focus on how our system and their system is different. And that is why it's important to talk about the human rights issues and the kinds of pressure that the Chinese government can bring to bear on individuals, especially, as you had mentioned in your opening statement, whose families are still in China.

Now, I think it is a really delicate balance. And so some of these reporting programs, and also just following up on different affiliations and thinking through the risk matrix is one of those tools that can be very useful because all resource does not have the same amount of risk, right? And so, it's important to not have a one-size-fits-all approach to this. But it also highlights the importance of really investing in homegrown talent as well.

Thank you.

Senator BARRASSO. So Mr. Turk, more than a year ago, I wrote to the Department regarding the persistent threat of the Chinese foreign nationals doing research on sensitive technology at our labs. A copy of the letter (holds up copy).

I brought to the attention that 162 Chinese nationals actually stole sensitive research material from Los Alamos and the lab. Your Department, again, answered the letter, but really didn't answer my question. So let me ask the question to you: Does the benefit of the work of the Chinese foreign nationals within our labs outweigh the documented risks to both our research and our national security?

Mr. TURK. Let me first thank you for all your focus on this issue. Thanks to Miss Puglisi and others who have focused their careers here. And I thought that Miss Puglisi's testimony, as I said in my opening, was incredibly useful, just eyes-wide-open, right? Here is the threat and here is what we face and how do we deal with it and get the balance right. So three things, maybe just to point out, and happy to get into this in any detail. One, we do have specific restrictions. So you can't work at a DOE lab if you have done a talent recruitment program. And to make sure that we have that prohibition and those restrictions in place and trying to really think about not just what is called a talent recruitment program, but other ways that the Chinese government or others can get around that as well so that we have that eyes-wide-open on those specific prohibitions.

Secondly, as was mentioned, we have the science and technology risk matrix. This is going beyond what is under export control or what is under classification and making sure we are looking at technologies. And just as Miss Puglisi said, doing a ranking of where are the most are sensitive technologies. AI is one of the six sensitive technology areas that we have a particular focus on in this risk matrix. And make sure that for those very sensitive applications, we have extra protections. So it is a risk-based model along those lines.

Third, we do have a counterintelligence unit at the Department of Energy, and all of our field offices cover all of our labs. So we are actively investigating and making sure that we are following up on any leads so that we can be as thoughtful and proactive as we possibly can. There is a balance here, just as you said, just as Miss Puglisi said. It is a great part of our scientific apparatus that we have folks from all over the world who want to come work here, right? Leading scientific minds, who, you think of Albert Einstein. You think of a number of others who benefited our country immensely, and we want to take advantage of that, especially where appropriate with open science with areas that are fruitful for that kind of focus as well. It is also useful to note, I have one statistic

here—many of the folks who come here to work in the U.S., including in our labs, end up staying and becoming incredibly important parts of our ecosystem. So over 90 percent of top AI Ph.D. students from around the world stay here in the U.S. five years after graduating. And that is a huge benefit, but looking forward to working with you further.

Senator BARRASSO. I appreciate it because the good news is 90 percent come and stay and then the concern is that there is potentially the ten-percent that do return to China.

Mr. TURK. Absolutely, or have families there, as you have mentioned, and Miss Puglisi has mentioned. And again, eyes-wide-open to take those threats head-on.

Senator BARRASSO. Yes.

Dr. Stevens, I don't know if there is something you want to add on this, but I am interested in how foreign nationals from countries of concern, how they are vetted before they are hired in your lab?

Dr. STEVENS. There is a process that is actually quite similar across all the laboratories where there is a background check. There are the filters that Secretary Turk mentioned in terms of recruitment programs and their history. There is a famous form—493, we call it—that foreign nationals have to fill out. So it's a long process to get hired and get cleared. And not just to be hired, but even to come as a visitor and to participate and use our facilities. So I think the labs do a quite good job of screening this and they make very valuable contributions. One statistic that I think was maybe mentioned is that over 60 percent of the computer science graduate students in the U.S. are foreign born. And the workforce component that we need to build advanced AI systems will not function if we prohibit those students from participating in this ecosystem. So we are going to need to really accelerate our workforce development, and foreign-born participants are an important component of that.

Senator BARRASSO. So then, a follow-up to that to Mr. Wheeler. So given the global nature of the technology development, how does your organization navigate the challenges of international collaboration while ensuring the security and the integrity of the research?

Mr. WHEELER. So, much like the national labs, we have a process for how we onboard talent as well. We also have, you know, ongoing training that is mandatory. It's around global trade, and so it's very specific. Everyone gets trained around, you know, what are the regulations around how do you interact if, you know, whether it's a collaboration opportunity with anyone abroad, honestly. And so, we have very strict control that manages what kind of technology can be transferred, who we work with, so very tight guidelines there. And then above and beyond that, for the projects we are involved in specifically, you know, and this is obviously closer to Department of Defense, but you know, if it's a project that requires only cleared personnel, we have that ability. We have the ability to do secure manufacturing. So we have a lot of steps in terms of security and who we work with and then how the work ultimately gets done.

Senator BARRASSO. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Hirono.

Senator HIRONO. Thank you, Mr. Chairman.

So we have heard from all of you that the Chinese government has a systematic campaign of stealing American intelligence—intellectual property—to advance their economy and that our DOE labs are targeted for this kind of effort. But I want to point out, as some of you have pointed out, the sensitivities involved and the balance that is required. So it is important to deter Chinese government wrongdoing and prosecute espionage and theft, but our concern is about the Chinese government's actions, not Chinese people. And we must avoid misguided prosecution such as what was undertaken by the Justice Department in the previous Administration with their China initiative. Going after researchers on shoddy evidence will hurt, not help, American innovation by sending the best minds elsewhere.

So listening to some of the responses that you have provided already on this subject, for Secretary Turk, you say that we are going forward with eyes-wide-open and we have some proactive steps that the DOE has taken. So do you consider these steps to be adequate to protect us from the kind of intellectual property espionage engaged by entities such as China, and perhaps Russia and Iran?

Mr. TURK. Well, you are right to say it's not just China. There are others as well, of course—Russia, Iran, North Korea, et cetera. And I think the short answer and the honest answer is, we always need to do more, right? The threat is evolving and we need to evolve our responses accordingly, which is why I mentioned this risk matrix. We are annually updating that risk matrix now so that we make sure that we are updating in terms of what technologies we consider sensitive, what protocols we have in place. We have a standing group now made up of folks from throughout the labs and DOE headquarters to take a look and continually provide ideas to the Secretary and myself so that we can continually improve. So we just need to improve on a regular basis, on a continual basis. And as you say—rightly—get that balance right.

Senator HIRONO. Because with the China initiative, I would say that we did not get the balance right. And in fact, the message to the Chinese community and the AAPI community was that here is our government targeting these people, and it created an environment where AANHPI people were targeted for various kinds of abuse, to say the least.

For Dr. Stevens, in the wake of the devastating fire on Maui, residents have been subject to disinformation on social media, likely coordinated by foreign governments, governmental entities, and generated with AI to discourage residents from reaching out to FEMA for disaster assistance and to sow distrust in the Federal Government. Are you aware that this happened in the wake of the Maui disaster?

Dr. STEVENS. Absolutely.

Senator HIRONO. Yes, so, you know, at this point, and with more of these kinds of natural disasters occurring with much more devastating results, we can expect that there will be, probably, these kinds of misinformation to sow distrust in our own government. So how can we use AI or other tools to rapidly detect and counter such efforts to spread disinformation, especially in emergencies or following disasters?

Dr. STEVENS. So I think we have to take several steps. One is to have advanced systems for detection of synthetic or deep fake information, right, non-true information that gets disseminated. We should uphold the existing laws that prevent that kind of information legally from being disseminated through social media channels. We need to enforce watermarking, this technique of putting secret information in AI-generated output so we can detect when it's generated by AI. And we need to make headway on watermarking official sources, that is, official news that comes from governments or from responsible parties so that it can be detected automatically that that is true and correct information coming out, and distinguish it from misinformation generated by AI. So there is a multiple-layered approach to protecting the citizens from disinformation. We have to do all of those things.

Senator HIRONO. Do you think, Secretary Turk, that we already have these kinds of systems in place, because, as I mentioned, these kinds of natural disasters are occurring more frequently with more devastating results. You can't have all this misinformation out there stopping people from accessing the very kind of help that they need. Do we have these kinds of counter systems already in place?

Mr. TURK. So honestly, we have some of them in place, not just at Department of Energy, but others across the government, but not as much as we need to, absolutely. And Professor Stevens, I think, is exactly right. We need a layered approach and we need to continually update and improve that, and frankly, have the capabilities, like we are talking about in this FASST proposal in the U.S. Government so that we can do the kinds of monitoring, we can do the kinds of analysis that allow us—not only the Department of Energy, but others across the government—to have the information and the tools to do the watermarking and other mitigation efforts.

Senator HIRONO. Do the other two panel members want to weigh in on this concern that we have following disasters, that there are entities such as Russia that are spreading misinformation to people who are already in great pain?

Do you agree that we need to put in place ways that we can counter this kind of misinformation?

Ms. PUGLISI. Right. I think the challenge of misinformation with these tools, as I mention in my written testimony, with the recent reports about what was happening with Facebook and other kinds of social media, we see misinformation across a wide range of topic areas, from the natural disasters to, as I mentioned in my opening statement, all kinds of activities that the U.S. Government are either doing or putting in place. So I think it's a growing issue.

Senator HIRONO. Yes. I want to note that in the case of Maui, the family of federal agencies were there, over 25 or so agencies with over a thousand personnel, and yet, there was all this disinformation out there saying that the response was lacking. And so, this kind of sowing of mistrust by—I would say Russia was a big actor in this instance.

Once again, for Dr. Stevens, I just want to note that your testimony highlighted some of the ways that AI can provide breath-taking opportunities for technological innovation, but what are Argonne and the other DOE national labs doing to ensure that the

technologies you are helping to develop are accessible to small businesses to help them innovate?

Dr. STEVENS. So we are very concerned about the availability of small businesses and students and so on to learn about AI and to use AI. I think this concept is often called democratization of access. The different DOE labs have different programs to make access to our computing facilities and AI models that we produce, that are open, that are safe and secure, available to those communities, and we provide help for those communities, whether it's small businesses or whether it's local governments, to gain access to our systems to do that, and I think it's an ongoing effort. I think more needs to be done there. And I think DOE, working in concert with other agencies, particularly NSF, via something like the NAIRR initiative, could actually make a big impact on that. And that is something that we should do together.

Senator HIRONO. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Now we have Senator Murkowski.

Senator MURKOWSKI. Thank you, Mr. Chairman. Thank you for this hearing this morning—obviously a very, very timely topic. As was just alluded to in Senator Hirono's question, there is a lot of good that we can gain from AI, and as scary, I think, as it is in so many different areas, I think it's important not to lose sight that when utilized correctly, it can truly be transformational.

So a question to you, Secretary Turk. As we are looking to different applications for good within AI technologies and AI workflows, we talk a lot here in this Committee, and we have been talking a lot about things like permitting reform, something that has proven to be tediously long and involving multi-layers of government processes. Do you see application for being able to streamline some internal government processes so that we can reduce the time, for instance, that it might take for an agency to deliver on a permit, or to really just kind of process any paperwork, reduce workloads? How do you see this being utilized for the good?

Mr. TURK. Well, I think the short answer is, absolutely. We are sitting on a treasure trove of data from previous applicants for different permits out there. If we can harness that data with algorithms with AI, we can shrink the timelines for permitting. We can take advantage of that data in a way that allows us to do what we need to do, which is build out our electricity infrastructure, our transmission, other kinds of infrastructure that we need in our country. So there is no doubt in my mind, there is an awful lot of good that can happen in the energy space, including accelerating on the permitting side. We have got a lot of renewables coming into the grid. We have got to balance all of that. AI can be incredibly helpful with the power and the data that it has available.

Senator MURKOWSKI. So you have had an opportunity—a couple of opportunities—to come to Alaska. You have been read in very well as to many of the unique aspects. And unfortunately, one of the unique aspects that we have is sometimes we have a lack of data. We just haven't done the mapping. We haven't done the review, the analysis, and so, we know that with AI, your output is just as good as your input. And if you have these holes in that, it

can be a concern in itself. So how can—again—how can we utilize the benefits of AI in government processes for good while ensuring that, perhaps, some states, some areas, like Alaska, where data is just not complete, that they are not actually disadvantaged? Have you given thought to that?

Mr. TURK. Yes, absolutely. And let me say what a pleasure it has been to work with you and your staff. And I have had a chance to not only come up to Alaska and go to Anchorage, but also to get out there to Nome and Kotzebue and other areas and really hear from folks in terms of what we can do from the Department of Energy to try to be helpful in that space.

But I think you raise an incredibly important point. AI is only as good as the data that you feed into it. And if you don't have the data, it can't be the powerful tool for good that you just highlighted on that front. So I think it's a continuing effort on our part, and I am eager to work with you and our Arctic Energy Office to make sure that we are doing everything we can from the Department of Energy, working with others in the Federal Government, to make the investment so that we have that data available so that it can be feeding into these AI models. So it's an ongoing effort. We are trying to make sure that we are bringing that in to everything that we do, but it's an ongoing effort, and something that we will continue working on.

Senator MURKOWSKI. Well, we do need to work together on it. And as we identify—you know, I spend a fair amount of my time on the appropriations side with the Department of the Interior budget and recognize that we are still directing a lot of resources—federal resources—to just basic mapping.

Mr. TURK. Yes.

Senator MURKOWSKI. Just basic mapping. So we have got a long ways to go there.

Let me ask you about the Department of the Interior. About a month ago, the IG for Interior, Mark Greenblatt, noted in an op-ed in the Washington Post that there had been an inspection undertaken by his office and they were able to use a simple tool to crack more than 18,000—or 21 percent—of the department's passwords. And this included senior department officials, hundreds belonging to employees with elevated privileges. More than 14,000 of these passwords were cracked within the first 90 minutes of testing. And he noted that his office was able to do this by spending less than \$15,000. That should alarm all of us.

Probably a general question, and I hope you answer yes, but we understand what happened at Interior. Is Department of Energy any better prepared to ward off nefarious actors than we saw at DOI?

Mr. TURK. So we are trying to continually improve. One of the things that makes me most nervous, and you are right to point out the benefits of AI, but one of the biggest challenges—and the technology is only improving and improving—it makes it easier for less sophisticated actors to do more sophisticated kinds of attacks, whether it is cybersecurity or any number of other things—biohazards, even nuclear proliferation efforts as well. And so, we have to take that head-on. That is why we need to make the investments in the U.S. Government so we can detect these kinds of things so

we can be ahead of the curve as much as we possibly can. But this is something we need to keep working on day in and day out, whether it's the Interior Department, the Department of Energy, or private-sector companies as well.

And this should be a wake-up call. The Pandora's box is open. We now need to deal with it and we need to take these kinds of emerging AI challenges head-on. And we are not there. We are not there where we need to be. We need to make the investments. We need to keep working at this. This is why we wanted to put together a proposal, our FASST proposal, with our ideas of what we think we need to do to try to do what we can from the Department of Energy side, and again, have the back and forth with you, with others here in Congress, to make sure that we are as prepared as we possibly can be. But we have work to do.

Senator MURKOWSKI. We have work to do. My fear is, what we saw within the Department of the Interior is just one department of 12. And where the vulnerabilities may be a little bit different, but the impact can be equally—

Mr. TURK. Huge.

Senator MURKOWSKI. Equally disastrous.

Mr. Chairman, thank you.

The CHAIRMAN. Thank you.

And now we have Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you, Mr. Chairman. Thank you to the panelists for this great conversation.

Let me start with Deputy Secretary Turk, because in Nevada we have—and I want to thank, also, Hewlett Packard. They were a part of this. We have been having some red team hacking going on at some of our universities to really assess what is happening here. And let me address what everybody has talked about—the nefarious actors. The concerns here that AI systems can be tricked into providing instruction for causing physical harm. We have talked about that. We need to address it. I think we need to as well. I think those red team hacking weekends are just as important. That's the manual piece of it, I think, Dr. Stevens, you talked about, that we need to continue. And let me just highlight, because I know the weekend in particular that I am talking about in August in Las Vegas, it was designed around the White House's Office of Science and Technology Policy's "Blueprint for an AI Bill of Rights," and it's a competition that happens regularly.

But my question here is one, yes, that needs to continue. Two, though, it also is building our cyber workforce. Is that right? That's what is key to this as well is that we need to have more engagement in building that workforce. I am proud that UNLV was the host of this and will continue to be the host of these types of red team hacking exercises. But it also is part of this idea that we have to create these academic centers of excellence in cyber defense, which UNLV is, a number of colleges are. And I think many of you are participating in those exercises.

So I guess my question for you, Deputy Secretary Turk, is, what else should we be doing to build out that workforce? I know there is work going on right now. Can you talk a little bit about the National Cyber Workforce and Education Strategy? How does that fit in to what we are trying to achieve with developing that cyber

workforce, and what else do we need to know here in Congress to support it?

Mr. TURK. So the workforce piece is absolutely indispensable, and I think there is a number of ways we need to come at it. We need to have a comprehensive and coherent strategy to it. First of all, if you want to have top talent come into the government, for all the functions that we need to serve, you have to have the cutting-edge facilities and capabilities, right? The fact that we have the world's largest supercomputer is a pretty nice attractor for some of the top talent wanting to do cutting-edge applications along those lines. We have the data. We have the other pieces as well. So we have to have that infrastructure that is attractive for that top talent.

The private sector is going to be able to pay folks an awful lot more than the government, even if we have bonuses and other kinds of attractive options, which we are trying to do. Having the national lab apparatus gives us greater flexibility, candidly, than if they were all Federal Government officials in the civil servant kind of sense. And so, I think—and Professor Stevens can certainly talk about that—using those partnerships. Argonne National Lab has a partnership with the University of Chicago—cutting-edge university there. That helps in incredibly important ways to try to channel as many folks as we can into this sector.

But I think there is no way we have a successful AI strategy as a government, as a country, unless we have the workforce and the pipelines for the workforce, making sure that we have that capability, not just in the private sector—incredibly important—but in the government for all the functions that we need to have here.

Senator CORTEZ MASTO. And as we are building out that workforce, and I am going to ask Hewlett Packard, if you can, because I know you were part of this and you have—Hewlett Packard has a Future of Work Academy for community and technical colleges and they are involved with nearly, I want to say, 100 institutions and over 500 students. And so, the private sector is engaged, correct?

Mr. WHEELER. Absolutely. In fact, I am glad you even mentioned the centers of excellence because what we have found over, you know, the years—honestly, decades—is that really is a best practice for, you know, once you have, you know, a center with maybe with the compute capability, but you bring together, you know, those domain experts that are local to that institution, you know, you bring the universities that are local there as well. And it really does allow you to develop that local workforce. And as we think about AI and needing more and more of that expertise, it's a great best practice to, again, help develop that workforce locally and just, you know, kind of grow and innovate together.

Senator CORTEZ MASTO. And this is the opportunity, and maybe, Dr. Stevens, I am going to ask you to talk about this, because it is so hard for us in Congress to come back in and overlay a framework and then actually try to develop values and principles in that framework. And this is an opportunity, as we are building out that cyber workforce, to grow those values and principles around AI. Is that the goal here when we develop the curriculum?

Dr. STEVENS. Yes, absolutely. I mean, as AI becomes more powerful, as has already been mentioned, it does two things. For somebody who knows something, it empowers them to do more, right? So whether that is somebody who is defending our systems from a cybersecurity standpoint, it allows them to be more powerful, to affect more systems, to be smarter about how they can do defense. But it also empowers the other side to be more aggressive in how they might attack systems. And we need to, of course, win those battles and we have to create a community and a new way of thinking—an AI-enabled cyber strategy. And I think that is what we have to start teaching.

And of course, it's very attractive to the students. When you talk about cybersecurity, they are already interested, but then you bring AI into it, and they are super-interested. So I think we have a big opportunity to bring more people into the workforce on this by attaching it to the AI agenda.

Senator CORTEZ MASTO. Thank you.

Ms. Puglisi.

Ms. PUGLISI. And that is really an essential part—the workforce in the future competition. And I might add that it is also—we have spent a lot of focus on looking at that Ph.D. level or higher education level. It's really, what does it take to have that technically proficient that does not necessarily need a degree or need an advanced degree. And I would venture to say that it's really important to start and begin that at the K–12 level and really lay that groundwork because that is really what it's going to take to compete.

Senator CORTEZ MASTO. And that appears to be what is happening with what I see with the different competition, the different—

Ms. PUGLISI. Right.

Senator CORTEZ MASTO. Whether it's the Federal Government, state, or private sector, that is the focus.

Ms. PUGLISI. Yes.

Senator CORTEZ MASTO. Correct?

Ms. PUGLISI. Yes, and actually CSET has done a lot of work around those topics and the importance of competitions as well as looking at the demographics of that workforce.

Senator CORTEZ MASTO. Thank you.

Ms. PUGLISI. So we can make sure that you have that. Thanks.

Senator CORTEZ MASTO. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

If we could, I will tell you, we have votes—two votes—at 11:45. We got to keep our questions—I know we went to seven. We will go back to five minutes, if we can. If you need a little bit longer, fine. If you can stay closer to five, that would be great.

Senator Hawley.

Senator HAWLEY. Thank you, Mr. Chairman.

Mr. Turk, since I had you before me the last time we talked, we talked about the radioactive contamination that the Federal Government had delivered to the St. Louis and St. Charles regions of my state, and in particular, we talked about Jana Elementary School in the Greater St. Louis region, which was then and is now

currently closed because of nuclear contamination that private tests found were in the school. Now, when we visited last—this was in February—you told me that you were having conversations about it. I am just looking at the transcript here. I asked you about the letter from the Hazelwood School District to the Department of Energy requesting additional testing. You said, “I have seen their letter. We have talked about it.” You said, “we are having conversations, including with the Army Corps.” You said again, “we are having conversations with the Army Corps.” When I asked you what you are going to do, you said “I will talk to the team.”

So that has been multiple months ago. Why don't you give me an update? What is the Department of Energy doing?

Mr. TURK. Yes, happy to do so, and we have a response letter to your most recent letter.

Senator HAWLEY. I have read it.

Mr. TURK. It should be coming today or tomorrow that I was just—

Senator HAWLEY. I think you sent one yesterday. Well, good, maybe there is more.

Mr. TURK. There is another one as well. There are two.

Senator HAWLEY. Good.

Mr. TURK. And there is a second one that should be coming today or tomorrow that I spent some time with the team reviewing and making sure we are trying to be as responsive as we possibly could on that front.

The Secretary, myself, the head of our legacy management team, Carmelo, is working with the Army Corps and others on this front. And on the testing side, in particular, I have pushed the team several times. I have said, what can we do? Is there something we can do from the Department of Energy side? And what we can do is work with the Army Corps, and we are happy to be very active with the Army Corps and make sure that they are doing, under their authority—FUSRAP gave the authority for these clean-up sites to the Army Corps. We are playing more of a supporting role, but we are happy to not only play that supporting role, but to try to push and work with our interagency partners to be responsive, certainly, to listen to the concerns that you have expressed, the concerns of the community. It's a horrific situation. I am a parent and I have three kids. If this was happening in my school, I would be certainly nervous. If I was a school a few miles away, I would be nervous as well.

So there is an awful lot that we need to do, not just on the science, but also on the human element as well. And thank you for all your focus on this very important issue.

Senator HAWLEY. Well, when you say that you are happy to do it—to do X, Y, Z—the work with the Army Corps, are you doing it? Are you pushing them to do the additional testing?

Mr. TURK. So we are having active conversations with the Army Corps.

Senator HAWLEY. That's what you said in February.

Mr. TURK. Well, it's for them—because it's under FUSRAP for them to make the decisions about where they think it's appropriate to do additional testing. We have had active conversations. We are having conversations about what more they are doing right now,

and they are doing more right now. I will let them talk to you about other testing that they are doing.

Senator HAWLEY. Oh, I am aware of what they are doing. Listen, let me tell you what the situation is. Just a few days ago, the Army Corps reported that they have removed 301 truckloads—301 truckloads—of radioactive dirt from the bank of the creek that's right near the elementary school. Now, this comes after they said for months that there was no contamination anywhere near the elementary school. That's what they said to the community, that's what they said to the parents, that's what they said to the school district. And they said they would not do any more testing. It was your responsibility to do the additional testing. You said, no, it's not. It's their responsibility.

So currently nobody is doing anything more additionally. And this is not just a few months, Mr. Turk. This is 70 years. Since 1949—1949—there has been contamination, radioactive contamination in the water, in the soil, all over the St. Louis region. That is a heck of a long time. And for 70 years, what we now know, we discovered even since you and I talked last, because of the efforts of St. Louis residents who got FOIA materials that show that the Federal Government knew from the 50s and 60s forward that there was significant radioactive contamination and they did nothing about it and they systematically misled and lied to the residents of St. Louis and the St. Charles region and said, no, it's actually—it's okay, play in the creek, it's fine. There is nothing we can do here. So it's just the same old story over and over. So I don't want to hear about conversations. I want to hear about action. I want that school re-opened.

Now, tell me about the Weldon Spring site, which is another of these nuclear contamination sites. You have total ownership of that. When is it going to be fully remediated?

Mr. TURK. So the response that we have for you lays out the history, and we have—

Senator HAWLEY. I know the history. Tell me when it's going to be remediated.

Mr. TURK. And if you look back in our archives, of course, the Department of Energy was created in the 70s, but we have precursor agencies that were responsible for the kinds of time periods you are talking about, and we lay that history out, just from our records. But we are happy to go into any level of detail in terms of what the government did or did not do at 20, 30, 40, 50 years ago, at least based on our record along those lines.

We are very focused on the creek. I have a map here right in front of me, looking at all the schools and others in the vicinity of the watershed in the creek area, and have asked our legacy management team, which is the responsible—

Senator HAWLEY. But when is the Weldon Spring site, which is squarely under your jurisdiction, when is it going to be remediated?

Mr. TURK. So we will have to get back to you on that. I don't have the exact data on that.

Senator HAWLEY. Oh, for heaven's sake. Did you not think I would ask that today? I mean, I have written to you about it multiple times.

Mr. TURK. We are happy, Senator, whether in a hearing or frankly—

Senator HAWLEY. But this is how this goes—you were before me in February and you said I will have a bunch of conversations, I will get back to you. It's September. Now you are saying I will have a bunch of conversations. I will get back to you. Are we going to be having this conversation again in six months, or nine months?

Mr. TURK. No, I can get you that information today. I just don't have it right in front of me.

Senator HAWLEY. Good. Today would be good.

Mr. TURK. I could get it back to you today.

Senator HAWLEY. Good. I will hold you to that. And I am glad we are in an open forum here.

Mr. TURK. Right.

Senator HAWLEY. So let's get that done and let's get a date fixed on when the remediation of Weldon Spring—and for those who are wondering why he was talking about an elementary school a second ago, and now there is this other side—yes, that's because there are multiple sites in the St. Louis and St. Charles regions affecting thousands of people for over 70 years who have been exposed to this contamination and lied to about it. So yes, I am not happy about it.

Last question for you. I recently submitted an amendment to the National Defense Authorization Act that would provide compensation to the victims of this nuclear contamination. I am delighted to say it passed the Senate, and as I look across the dais here, just about every person on that side of the dais over there voted for it. I thank each of you. Thank you for it. Senator Luján and I worked together on this. The President, President Biden, has said that he thinks it is vitally important to get these folks compensated for what has happened to them.

Do you agree with that? Do you support our legislation to compensate the victims in St. Louis and elsewhere of nuclear contamination and radioactive waste?

Mr. TURK. So I certainly support the intent behind the legislation. It's the Department of Justice that's the relevant agency here. So I can't speak for them or speak for the Administration as a whole on—

Senator HAWLEY. You won't agree with the President?

Mr. TURK. What's that?

Senator HAWLEY. You won't agree with the President?

Mr. TURK. I will always agree with the President.

Senator HAWLEY. Okay. Well, let me ask again. Do you support the legislation—

The CHAIRMAN. Senator, can we hold—

Senator HAWLEY [continuing]. To compensate the victims of this nuclear contamination and radioactive waste?

Mr. TURK. Again, I will leave it to the President to speak about Administration policy on this. I have not seen what he said—

The CHAIRMAN. Senator, if you want to follow up with a second round, we will let everybody get their first round in. We will come back, okay?

Senator HAWLEY. Thank you, Mr. Turk.

The CHAIRMAN. Thank you.

Senator HAWLEY. Thank you.

The CHAIRMAN. Senator Cantwell.

Senator CANTWELL. Thank you, Mr. Chairman. Thanks for holding this important and timely hearing. Over the recess I held an AI forum in Seattle. Pacific Northwest Laboratory showcased its Rapid Analytics for Disaster Response, a tool that is a detection system for all hazards, and importantly, it was used to assist in both Ukraine and in some of the Maui aftermath. Others in the Allen Institute for AI environment have demonstrated how they are using satellite imagery to improve wildfire management—really important for us in the Pacific Northwest. Also using it to detect illegal fishing in our maritime sector, a very important issue to us in the Pacific Northwest, and enforcement and surveys of our land for conservation purposes.

So we need to invest, I believe, in more innovation, and that is why we, obviously, are supportive of what happened with CHIPS and Science and now with AI for our competitiveness. The United States cannot slow down on AI as it relates to our competitiveness internationally and for national security reasons. So our national labs have assisted us in supercomputers, reliable and robust datasets. U.S. Department of Energy international labs are essential to our leadership in artificial intelligence. So I wanted to ask our panelists—you spoke about the need for U.S. leadership on this issue—Deputy Secretary Turk and also, I believe, Dr. Stevens, you mentioned that lab supercomputers are positioned to create the tools for risk assessments to evaluate AI systems. So how do we get both NIST and DOE working together on these tool assessments in determining what are true risk assessment, so they are identified, and what do we need to do to help build a workforce, particularly in skilling the workforce for AI? And either one, Dr. Stevens or Mr. Turk, either one of you want to start? It doesn't matter.

Mr. TURK. Go ahead, Professor, you start and I will then bat cleanup.

Dr. STEVENS. So we are having good conversations with NIST about partnering in how to take the assets of DOE and connect them to the analytical and conceptual framework that NIST has been working on for AI risk management. So I think that is an ongoing conversation. They are participating in working groups that we have established, consortia across the laboratories that are working on how we will do risk assessment for large AI models. So I believe that part is already moving, and I feel quite positive about where that is going.

In terms of the workforce, I think the young people are hungry to work on AI. You don't have to encourage them. All you have to do is say "here is an opportunity" and they are there. I mean, our courses—any course at any major university that is on AI is going to be oversubscribed. So I think what we have to do is we have to provide enough resources that any student in the U.S. who wants to make a meaningful contribution to AI in the national interest has an opportunity to be funded to go to school, to go to graduate school, to do internships, and to participate. And that is going to require multiple agencies cooperating on that. DOE, of course, supports students and supports student internships, but in a very limited number. NSF, of course, can do it in a much larger number,

but other agencies as well. We need a coordinated, national strategy to build an AI workforce, and we need some leadership to organize that.

Senator CANTWELL. Okay.

Mr. Turk.

Mr. TURK. Yes, just two things to add. One—boy, what a gem we have when it comes to AI and everything else in the Pacific Northwest National Lab, whether it's some AI on a drought study or with vaccine development, there is example after example coming out of that lab, of course, working with Argonne and others of our national labs as well. I think the interagency partnership here is going to be absolutely key. Professor Stevens outlined what we are doing with NIST and we need to do even more with NIST on the risk framework along those lines, but it's NOAA, it's agency after agency that we have good partnerships with. And I think because we have the exascale computing power, because we have data, because we have these other facilities that you, not only with your role in this Committee, but your role as Chair of the Commerce Committee, as well, have been working for so many years to make sure we have these capabilities that can help work with partners throughout the interagency. And we just need to leverage that. We need to take full advantage of that.

Senator CANTWELL. And do you agree with Dr. Stevens about the workforce issue?

Mr. TURK. Completely agree, and rightfully for you to focus on this. Senator Hirono asked questions about this. We all need to focus on the workforce. And I know I have talked to a number of folks, they want to work on AI and they also want to work—the private sector is great and we need talent in the private sector, but they also want to work in the government and take on some of these public challenges as well. We just need to make it attractive to them in all sorts of ways so that we can compete.

Senator CANTWELL. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Hoeven.

Senator HOEVEN. Thank you, Mr. Chair.

Secretary Turk, you note that China is, you know, working very diligently to copy and take a lot of the capabilities and research that is being developed at our national laboratories. How much, in your opinion, how much have they taken or copied, and are the national labs really able to protect themselves, not only in terms of the information they have, but also as they hire people? Don't they have to be very careful whom they hire and how they hire and so forth so that they know that, you know, that information is not going from employees to China or other actors that, you know, have adverse interest to our country?

Mr. TURK. Well, thanks for the question. And the answer is, we need to be very aware and we need to have a layered strategy to deal with these security challenges. So we have put in place specific prohibitions. If you have worked in a foreign talent program in China, for instance—but it's not just China—then you can't work in a Department of Energy lab. So we have specific restrictions in place where we see particular risk. Secondly, we have adopted and now we are annually updating something called our science and

technology risk matrix, which looks at particularly sensitive technologies. AI is one of the six particularly sensitive technologies that we do an extra screening on and make sure that we are taking care of those sensitive technologies in particular. And then, third, we have also got counterintelligence experts in our field offices to cover all of our national laboratories that are looking into any allegations and making sure that we are running down all leads along those lines.

But we want to attract top talent in our U.S. national labs. We want to have that expertise coming and we benefit from that—public and private sectors. Many of those—over 90 percent of AI Ph.D.s who come and work in our labs and come and get their Ph.D.s here stay more than five years. So we benefit from that, but we have to have eyes-wide-open and have a real balance here so that we try to get it right and update it over time, too.

Senator HOEVEN. Well, you kind of went right into my next question, which is then what about people that leave, get recruited away, you know, because they have got all that incredible knowledge. And what if they get recruited to, you know, either a rogue actor or a country like China or somebody that is trying to get the information that way? They are just hiring them away from you.

Mr. TURK. Well, and it's not just happening with Chinese nationals, it's other countries' nationals who are being recruited—

Senator HOEVEN. That's true, not just China.

Mr. TURK [continuing]. Elsewhere also.

So we have to be eyes-wide-open on the front end, right, if there is a particular risk of an individual that we think could take some of their experience they learn in a national lab and take it back to China or take it to Russia or other countries that mean us a challenge in the world, then we have to have restrictions, and those kinds of screens in place, just that I mentioned, along those lines. And then, we have got to, you know, balance the benefits that we get from all this world-class talent coming here with the risks that we are going to have from some folks deciding that they want to go work elsewhere, they want to take what they learn and take it elsewhere. So we just have to be very vigilant and have a very layered approach.

And we have empowered a group of experts across the labs and headquarters to make sure that we are continually improving, not only our risk matrix, but how we do things more generally.

Senator HOEVEN. Yes, a real challenge, no question.

Mr. TURK. It's a real challenge. There's no doubt about it.

Senator HOEVEN. Because you need the talent, but you have to screen it on the front end. You have to be careful not to lose it on the back end. I mean, incredibly difficult.

Mr. TURK. It is incredibly difficult.

Senator HOEVEN. Along, kind of, in a similar way, but a little bit different, I want to ask both Ms. Puglisi and also Dr. Stevens, what about people just flat-out copying? Okay, so you develop some great AI product, whatever. How about somebody just taking it and copying it? I mean, we see that with—look at what Iran's doing with drones. I mean, they obviously just—and other countries too, just copying our technologies. It may be inferior, but they are just copy-

ing it in many respects. How do you prevent rogue actors from doing that kind of thing? Or can you?

Ms. PUGLISI. That is correct, Senator. It is a very difficult challenge.

Senator HOEVEN. I mean, China has made a living off copying and stealing our stuff.

Ms. PUGLISI. Right. And I would like to actually have a couple comments on your first question because I think it's important.

Senator HOEVEN. Sure. Well, with the permission of the—well, the Chairman is gone, so yeah, go crazy.

[Laughter.]

Senator HOEVEN. Go wild.

Ms. PUGLISI. They—

Senator HOEVEN. Exactly. We can do whatever we want now.

Senator KING [presiding]. I am sitting in for the Chairman.

Senator HOEVEN. Oh, okay. Take it all back, yeah.

Ms. PUGLISI. Okay.

Senator HOEVEN. Fellow Governor, we have got to mind our Ps and Qs.

Ms. PUGLISI. The copying piece is very much a challenge, but it is the technological know-how, I think. I think a lot of our existing mitigation strategies focused on things, right, something that is tangible. It is the technological know-how of how do you actually use that. So you can copy something or I can translate something, but I still don't understand what it means. And that is why that talent piece is so important. And I would venture to say that our system really is not set up for this particular challenge that we have today. We are pretty much—we are set up to fight the Soviets. We look for intelligence officers. We look for a direct military end-use and we have very narrow laws around economic espionage, which we could discuss en masse for a long time.

But what is being targeted are things that are earlier and earlier in the development cycle that are beyond most of our mitigation strategy. And that is going to be an ongoing challenge that we think about how do we find ways that we still enhance and keep investing in that early development cycle work, which is such an essential part of the DOE labs, while at the same time, you know, finding those ways to protect that. And then that kind of gets at the workforce that gets that technological know-how. It gets at how do we then, you know, find new ways to face this challenge?

Senator HOEVEN. I can tell you have been thinking about it. It's good you are very thoughtful about that and I appreciate that.

Ms. PUGLISI. Thank you.

Senator HOEVEN. I can tell it's something you are working on and that is good.

Thank you very much.

The CHAIRMAN [presiding]. Thank you, Senator.

We have Senator Kelly.

Senator KELLY. Thank you, Mr. Chairman.

Dr. Stevens, you know, we have been going through a sort of unprecedented period of drought in the West—worst drought, as far as we can tell, in 1,200 years. It has been going on for 20 years. This summer rather hot. You know, it is always hot in the desert, but we had an unprecedented number of days in Phoenix, espe-

cially, over 110 degrees and you know, we have had wildfires, unprecedented wildfires, not only in Arizona, but in other parts of the country and in Canada. These fires have had significant impacts, impacts on communities. And it has been clear to me that we have to leverage every tool at our disposal to mitigate these disasters, but also look for opportunities here to promote forest restoration, which has an impact on these. We have a big ponderosa pine forest in Arizona—biggest in the world, in fact. And we are looking to get this forest restored.

So obviously, the potential of artificial intelligence here, you know, can't be overstated with its ability to analyze large datasets rather quickly and accurately and to predict things. CAL FIRE is conducting a pilot program using AI to help with the early detection of wildfires. So my question to you is twofold. Can you first elaborate on the current initiatives and advancements here with using AI for wildland firefighting, if there is any going on?

And then, secondly, a little bit about looking ahead to how your laboratory envisions collaborating with other government agencies and the private sector.

Dr. STEVENS. Sure. So thank you for that question.

So we are quite familiar with the CAL FIRE effort, and our colleagues in San Diego have been very involved in building some of the technology for that. It is a really challenging problem. As you know, fires start with smoke, often, and AI trying to detect from cameras on mountaintops and from other vantage points. Early examples of fire often get confused by fog or by tractors stirring up dust or something like that. So there is a need to really improve the AI algorithms that are interpreting images, maybe to upgrade the technology so we can get both infrared imaging as well as visible light imaging and realize it is going to take some time to fully deploy AI and re-engineer how the processes in CAL FIRE and the whole teams will use that AI to be more efficient, right? Ultimately, the AI can put more computer-based eyeballs on the territory than humans could ever look at the monitors and so on, and so, I think the long-term impact of AI in firefighting and in disaster management, in general, is going to be huge.

AI can also synthesize and fuse information from remote sensing, from satellites, from on ground, from reports from people texting or tweeting or cameras and from the workers—firefighters on the ground into a common database that tells us exactly what is going on. And I think that is going to be critically important as we go forward to scale up firefighting efforts. The national labs have been involved in trying to model and simulate fire in the west, in particular. Los Alamos has had a very large program for many years trying to build simulations that would predict the likelihood of fires and to be able to, you know, understand the amount of flammable material that is accumulating through the forests and so forth. I think all the national laboratories are interested in helping with disaster management, and like the earlier comments about the work at PNNL, the work at Argonne, the work at Los Alamos and Livermore, everybody is really interested in this problem.

I think what we need to work out is how we partner between the federal and the state and local that often have the responsibility for this into a structure that really advances both AI, but also

takes a practical look at what—you know, we have to try lots of things, and not everything is going to work, and then adjust our strategy to focus on what works.

Senator KELLY. Do you know the specifics of the AI algorithm, and are they trying to incorporate lightning detection into it because—

Dr. STEVENS. The lightning—

Senator KELLY [continuing]. Obviously, a lot of forest fires start with lightning.

Dr. STEVENS. Absolutely.

Senator KELLY. And we know where lightning occurs.

Dr. STEVENS. That's right. So we can detect lightning through the EM spectrum, or through electromagnetic stuff, and overlay that on the geographical maps and then overlay that with imagery. So I am quite familiar with how that is being done, but I don't think it is fully integrated yet. I think we could actually do a lot better than we are currently doing.

Senator KELLY. Yes, because then you could just narrow the field—

Dr. STEVENS. Absolutely. If there is a history of lightning there and you are seeing smoke and—

Senator KELLY. Yes.

Dr. STEVENS. Exactly.

Senator KELLY. Okay, all right. Well, thank you.

The CHAIRMAN. Senator Hickenlooper, do you want to defer to Senator King?

Senator King.

No, Senator Hickenlooper. You all fight it out.

[Laughter.]

Senator HICKENLOOPER. Thank you, Mr. Chair. Thank you all for spending time here today. I think it's a fascinating discussion.

I want to start with Mr. Wheeler. We have a company in Colorado called Guild that does training for large companies, say, Walmart or Chipotle, that their employees want to take skills-based classes at colleges or universities or wherever. And Guild does polling of entry-level engineers and coders across professions. And recently, one of their most recent polls saw a dramatic increase, like near-universal, in the level of concern expressed at AI to these beginning level engineers and across every industry. And every industry, of course, needs technology. And I think this, you know, the intense computing resources that are needed to train and run AI models at scale raise a lot of questions you are already addressing. NREL, out in Colorado, operates a high-performance computing data center that is designed to be the world's most energy efficient. I think when we look at some of these things, what other types of efficiency can we look at, Mr. Wheeler, recognizing that there is a level of anxiety that has, you know, come up in terms of the workforce?

Mr. WHEELER. Yes, thanks for the question, Senator Hickenlooper, and I am very familiar with the facility and some of the machines there at NREL, being that Colorado is my home state. But I think there are multiple ways to look at this. So I think, as you say, all the excitement around AI—there are a lot of people wanting to get into that as, you know, maybe they are

transitioning careers, but understandably, you know, concerned with some of the risk around it. We have a, you know, something we say internally a lot is, you know, look, AI is not going to replace that scientist or that engineer, you know, editor, teacher, you name it, the list goes on. But those same individuals, those same professionals that harness AI and use AI will likely replace those that don't.

So that is why, I think, from a workforce and a transition, we are seeing many people wanting to get into that as a career. So they recognize the opportunity. And the great thing about Guild is, you know, maybe they are not taking people that historically came up from a STEM background or education, but guess what? With all the tools, everything that is being developed, you know, suddenly, you don't have to necessarily be the deep mathematics expert. You can be very proficient with the tool sets that are out there if you have that willingness to learn.

Now, that being said, you know, what are those guardrails that are in place or, you know, how do we think about some of the risk associated with the technology? You asked about, you know, what other things can be done. I think NREL is a great example of showcasing a lot of what can be done, whether it's from the energy recapture of those systems. As others on the panel have stated, just providing access to that type of infrastructure and compute is a big part of kind of lowering the barrier to maybe some of the anxiety, and being part of a solution because, you know, if you have a passion around that, as a field of study on how to, you know, mitigate, you know, some of the risk around this, well, having access, you know, enables you to, you know, develop and propose those types of solutions.

Senator HICKENLOOPER. Right. Thank you for that.

Ms. Puglisi, a lot of the innovations fueled by AI come from fundamental and applied research that is adopted by small businesses. And in your testimony, you highlight about how investing in research supports our country's technological leadership. How will the historic investments into translational research from the CHIPS and Science Act grow our technical workforce within our innovation economy?

Ms. PUGLISI. Yes, I think those investments are essential because I think what gets lost a lot of times are those transition points. And so, a lot of funding focuses on basic research, or focuses on applied, and I think that some of the advantages that are focused on in the CHIPS and Science Act are that it looks at those transition points and how do we move technology so that it best serves the public and best serves society. And so, having those kinds of skills, those are very different kinds of skills than actually doing the research, but having that support across what we call the Valley of Death, or other kinds of challenges, are really, I think, important to kind of keep that spark going.

Senator HICKENLOOPER. Great. Thank you on that.

Ms. PUGLISI. Thanks.

Senator HICKENLOOPER. I appreciate that.

And I will yield, and Senator King, I will wander over and make sure that that seat is covered if you take a couple extra minutes.

Senator KING. Thank you. Appreciate it.

Thank you, Mr. Chairman.

I wanted to put a fine point on this. A few minutes ago I put into ChatGPT the following question: "Write a poem about Joe Manchin and John Barrasso."

[Laughter.]

Senator KING. In less than three seconds, this is what it wrote.

The CHAIRMAN. Oh my God.

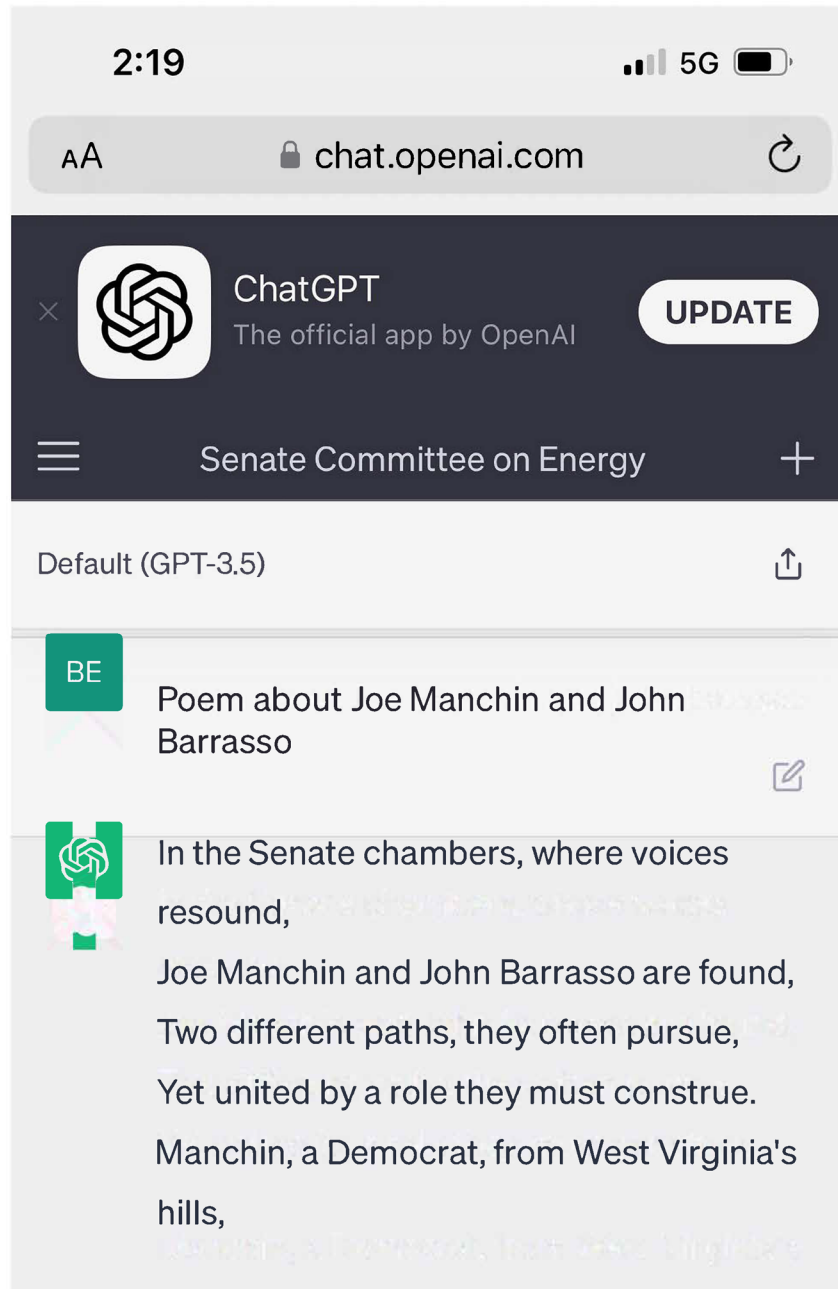
Senator KING. "In Senate chambers, where voices resound, Joe Manchin and John Barrasso are found. Two different paths, they often pursue, yet united by a role they must construe. Manchin, a Democrat from West Virginia's hills, his principles shaped by his home's coal-filled mills. He seeks compromise, a middle ground's grace, in a divided Senate, he finds his place. Barrasso, a Republican, from Wyoming's plains, with conservative values that deeply ingrain, his vision for policy, distinct and clear, in the halls of Congress, he perseveres. Though their ideologies often diverge, in the Senate they engage, discuss, and urge. For the common good, they both aspire, to serve their constituents, their hearts on fire. Two Senators, distinct in their view, yet bound by a duty to represent you, in democracy's dance, they play their part, Joe Manchin and John Barrasso, with determined heart."

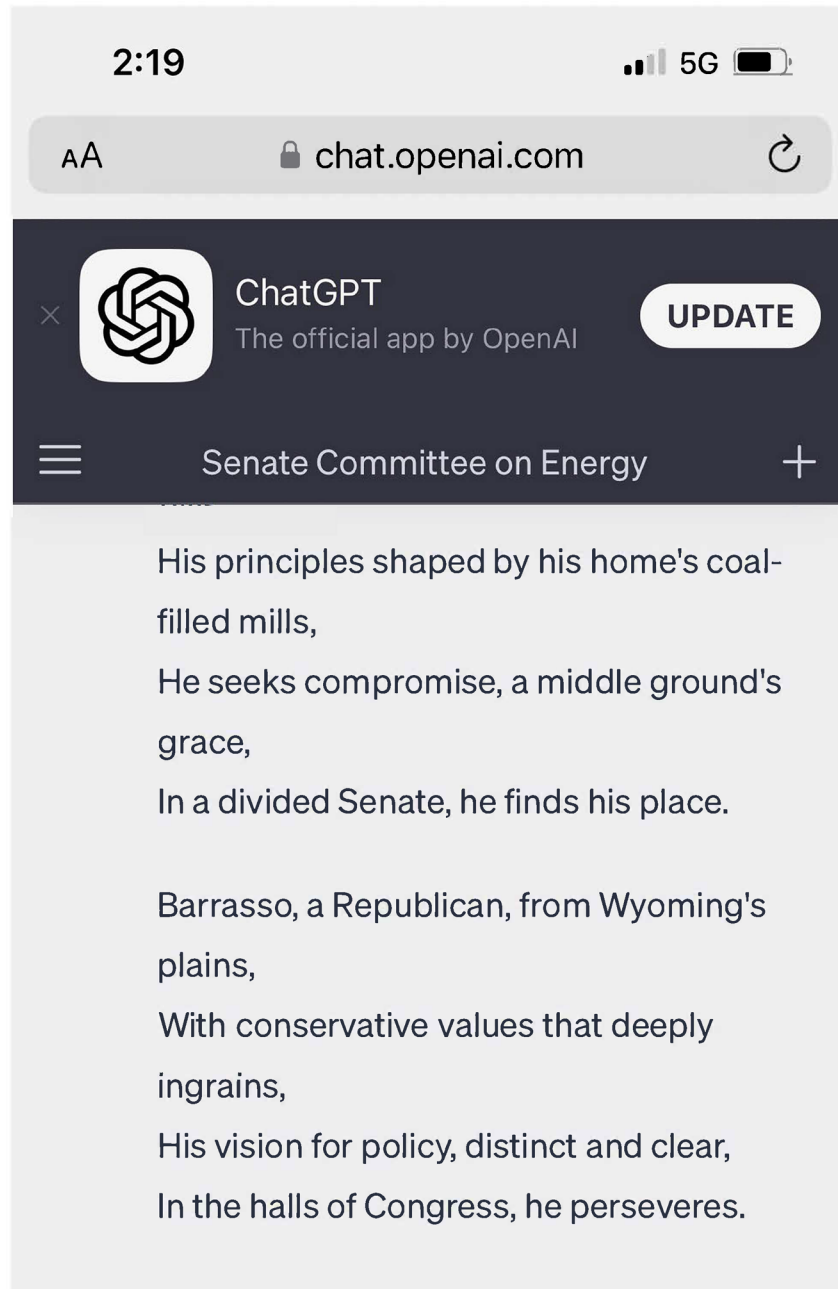
Isn't that——

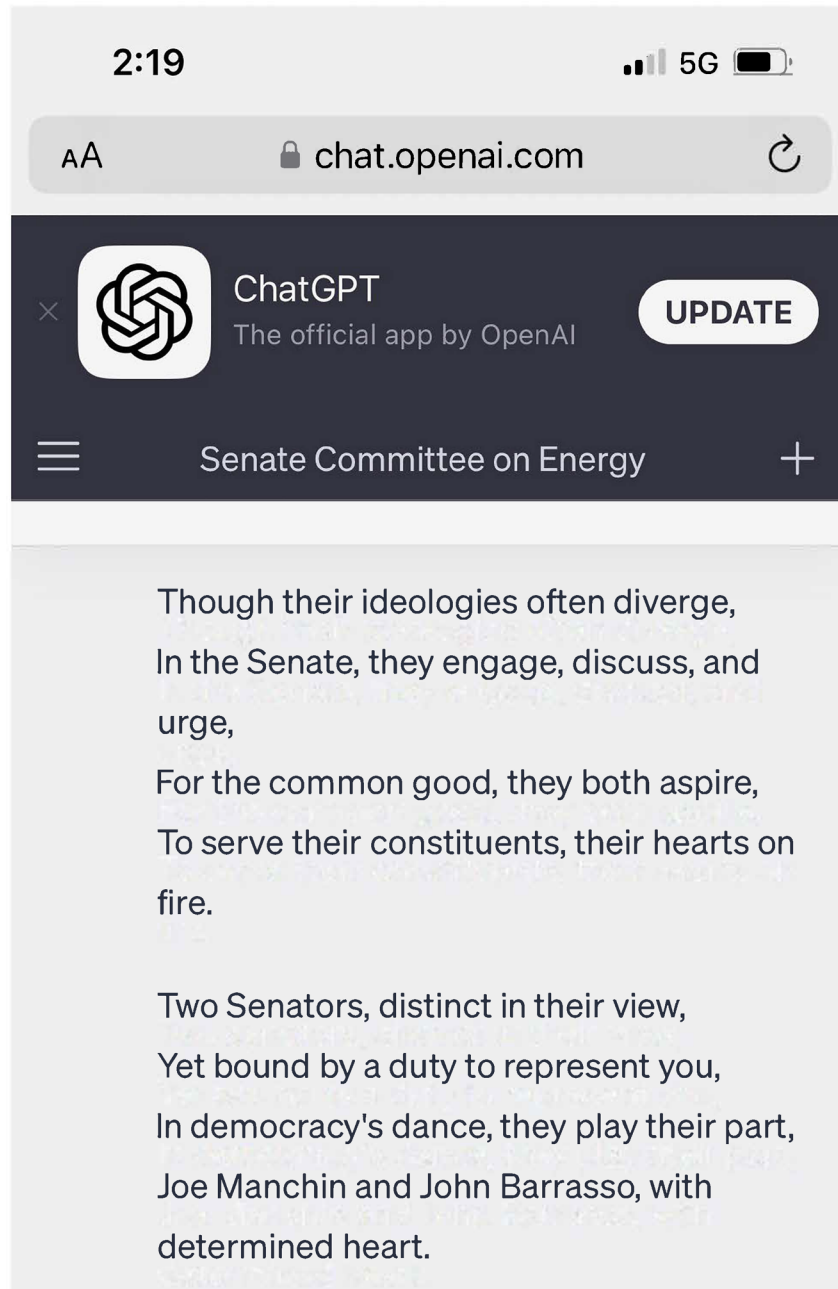
The CHAIRMAN. Let's make sure we don't eliminate that part of AI.

[Laughter.]

[Screenshot of the poem as generated in ChatGPT:]







Senator KING. But think of that. In less than two seconds the data that was searched to put that material together, make it rhyme, and have it be so representative of our two Senators. I just think we ought to realize the unbelievable power of this. That is sort of a homely example, but I think we need to understand the radical nature of this technology.

Mr. Turk, a homely question. One of the problems in the energy transition, which, as you know, is one of the major issues of our time, is ISOs' timeliness of processing applications for connection to the grid. There is a huge backlog in virtually all the ISOs in the country. Can AI contribute, because it seems to me that decision about interconnection, which would involve capacity, reliability, safety, that strikes me as an engineering question that AI should be helpful with.

Mr. TURK. Well, I think the short answer is yes. And I have been speaking to the heads of ISOs and really trying to make sure we are doing everything we can on the interconnection queue, which is a big deal right now, right? If you can't get things connected to the grid, then we are not going to achieve our goals. We are not going to get all the benefits from these technologies. So—

Senator KING. And right now, the queue is one of the major bottlenecks to this transition.

Mr. TURK. The queue and the queues with different ISOs is a major bottleneck. That is exactly right. And there are a number of efforts that are being undertaken right now. The FERC has put out some rules to try to make sure that it isn't just first in who gets consideration—it's first ready, so that we try to make sure that we are taking the applications of those who are most impactful along those lines.

Senator KING. I hope you will take steps to use AI to radically shorten this process. I think that would be a major contribution.

Mr. TURK. I think it would be great.

I wanted to highlight—there is an effort, the acronym is i2X, that our energy efficiency and renewable colleagues are working on that is using technology, among other things, to try to bring all the ISOs together in software fixes, AI fixes. Happy to get you more information on that, but it's a very exciting effort.

Senator KING. I appreciate that.

The word watermarking was used earlier. I don't want the government deciding what is true and not true. That is just not the way, the direction we want to go, and it's not consistent with our principles and values. On the other hand, it seems to me, people that use information, on the internet or otherwise, have a right to know its source.

Mr. Stevens, you mentioned watermarking. What we are really talking about is, for me, it's labeling. This film or this article was produced with AI. That would be important information for people to have in assessing the validity of what they are seeing. Is that—how close are we to having that technology?

Dr. STEVENS. We know how to do it. It is a question of getting agreement that AI companies would use some kind of common approach and not some proprietary approach because then how would we enforce or require it?

Senator KING. I was going to say, could the Congress require the platforms to——

Dr. STEVENS. They could, but——

Senator KING [continuing]. If they are going to post AI material, it's got to be labeled?

Dr. STEVENS. That is the current approach. I think it's flawed in the sense that there will be, ultimately, many hundreds or thousands of generators of AI, some of which will be the big companies like Google and Open AI and so forth, but there will be many, many open models produced outside the United States and produced elsewhere that, of course, would not be bound by a U.S. regulation. And so, I think what we are ultimately going to end up having to do is validate real sources as well as—we can have a law that says watermark AI-generated content, but a rogue player outside the U.S., say operating in Russia or China or somewhere, would not be bound by that and could produce a ton of material that would not actually have those watermarks and so, could pass a test perhaps.

So I think we are going to have to be more nuanced or more strategic in this, in that we are going to have to authenticate real content down to the source. Whether it's true or not is a separate issue, but if it's, you know, produced by real humans in a real meeting, that stream would get tagged so you would know that is real versus something that would be synthetic.

Senator KING. I am out of time and I am due over to preside, but I would really appreciate it if all of you would give some real thought to this because this is a current issue for us and we have got a major election coming up in little over a year. Disinformation via AI could play a pivotal role. We need your best thinking now. So to the extent you can get back to this Committee on these subjects, it would be very, very helpful to us.

Thank you, Mr. Chairman.

Dr. STEVENS. I am happy to do that.

The CHAIRMAN. Well, let me tell you, I don't need to tell you how informative and how interesting this has been, what we have received. I think everyone has told you what we are concerned about. My good friend here found something very complimentary, and I appreciate it very much, but he could have probably found something very concerning and harmful very quickly also.

I think the first line of defense that I am looking at that I am concerned about is how do we protect from altering people's lives? And that is basically their compensation, whether it be at their workplace or if they are retired—retirement checks, Social Security, Medicare. How well are we hardened there or basically preventing AI from figuring out a way to come through another door—back door, side door, anything differently that could put them at risk of changing and altering their lives, because that's when it's going to be very difficult to put that genie back in the bottle. And that's what I am concerned about. Getting in investment portfolios, you know, they are doing this all the time—trying, but it makes it very difficult. And it's bad enough when someone gets their credit card hacked and stolen and what they have to go through to get that corrected.

Can you only imagine what this could do?

So this is what we are asking all of you with the knowledge that you have and expertise, but also the challenges that we are going to have. I know we think about defense. We have been talking in Armed Services about offense versus defense. We are already using AI in defensive procedures now, but offensively we still want that human element involved to make a decision. Do we launch a strike or not? That is going to be very, very detrimental, and very important, and has unbelievable, far-reaching results.

So I think we are in uncharted waters to a certain extent, but those of you ahead of the curve right now can help us from falling, really, into the deep end where we can't be saved. So if you have learned anything about the internet, we learned that for all the good it did, there are people out there waiting to use it for nefarious situations, and they do it every day.

So with that, let me just say that I appreciate it very much. I think you all have done a wonderful job presenting this. You can see the interest that we have and the concerns that we have, but I think the support that you have from all of us, trying to make sure that whatever dollar we invest, we have to invest an awful lot. We are willing to do that. We just don't want to reinvent the wheel. We want to basically make the wheel run a little—balance it out and run a little smoother. So we are all here to help. But again, thank you so much.

Members will have until the close of business tomorrow to submit additional questions for the record.

Thank you, and the meeting is adjourned.

[Whereupon, at 12:00 p.m., the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

QUESTIONS FROM RANKING MEMBER JOHN BARRASSO

- Q1. What is the Department of Energy doing to ensure that technologies utilizing artificial intelligence remain unbiased and transparent, given the recent findings of bias in some platforms?
- A1. DOE recognizes the pressing need for scientific grounding in areas such as bias, transparency, explainability, data security and privacy, validation, and accuracy of AI platforms. We held a series of workshops with stakeholders across the innovation ecosystem to identify new and rapidly emerging opportunities and challenges presented by AI, culminating in the May 2023 release of the report AI for Science, Energy, and Security. The report identifies the importance of developing science-based verification and validation methods for AI models and the need for research into new methods for uncertainty quantification, explainability, and interpretability, as well as methods that quantify the information content of a training dataset. DOE has also published a digital AI Risk Management Playbook [<https://www.energy.gov/ai/doe-ai-risk-management-playbook-airmp>], a reference guide for AI risk identification and recommended mitigations to support responsible and trustworthy AI use and development.
- Q2. According to a recent GAO report, DOE has not assessed the resources it needs to achieve a fully operational insider threat program. Commercially available technologies now exist that can rapidly and accurately assess personnel, flagging those that require additional scrutiny while efficiently clearing others to get to work. Does DOE use real time risk assessment technology, or have a plan to do so? Can I get your commitment to have someone from your office brief my staff about the specific tools being utilized?
- A2. DOE is constantly assessing the required resources to achieve and maintain full operational capability with its Insider Threat Program, and we regularly review and assess the various DOE systems that may require monitoring. DOE utilizes available commercial technologies to review and assess personnel. Most, if not all, assessment technology is at a near-real time capability and DOE will continue to develop and work with other technologies to enhance that process. For more detailed information, a classified briefing may be required, and we can arrange a briefing on the specific tools DOE uses in its Insider Threat Program.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

QUESTIONS FROM SENATOR STEVE DAINES

- Q1. Deputy Secretary Turk, Tom Siebel, CEO of C3 AI recently wrote an article forecasting future impacts of pre-emptive regulation of AI. Mr. Siebel writes, "The effects of regulation will be to hamstring technological advancement, or worse, to criminalize science—to the advantage of our economic competitors and military adversaries." Do you agree the Department of Energy should refrain from supporting and enacting burdensome regulation that slows down our national AI development efforts?
- A1. AI is a dual-use technology, and the United States must maximize the opportunities presented by AI while also minimizing the risk of unintentional harms or intentional misuse. Many countries are investing heavily in AI in order to capture the technology's societal, economic, and national security advantages, and any efforts to regulate AI must be underpinned by deep knowledge of the technology itself. DOE has the expertise and capabilities to provide technical assistance that informs regulatory discussions; however, DOE's primary role will be to remain on the AI frontier, driving AI innovation for science, energy, and security.
- Q2. Deputy Secretary Turk, there have recently been many proposals in both the House and Senate to quickly regulate AI, a technology that is still in its emerging stages. Knowing that regulation will necessarily slow progress in the technological development of AI, as well as potentially help entrenched Big Tech organizations and keep smaller innovators out of the market, do you agree we should have light touch regulations and not stifle innovation?
- A2. Any regulation, particularly regulation of a quickly evolving technology, must be informed by technical expertise and driven by a deep understanding of the benefits and risks, including related to social and economic impacts. With expertise across open and classified research domains and existing partnerships with industry, DOE is positioned to provide its technical expertise and work with other Federal agencies to help manage the risks presented by AI while also maintaining our ability to advance our global leadership in AI.

The United States needs all sectors of society engaged in the advancement of AI leadership. This includes enabling innovation for companies of all sizes, researchers,

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

academia, and nongovernmental organizations – all key players in our innovation ecosystem. Community outreach and engagement with experts in the societal implication of science will also inform the responsible development of this disruptive technology.

DOE has successfully executed on analogous large-scale research and development efforts before, which have paved the way for American industry leadership. For example, the Exascale Computing Project has resulted in the U.S. operating the first openly-benchmarked exascale supercomputer, Frontier, which—like all of DOE's computing facilities—supports AI-coupled modeling-and-simulation workloads. The Exascale Computing Project, coupled with other substantial investments from the private sector, have led to the formation of new industries and enabled myriad innovations, and DOE and the National Labs are proud to continue this legacy.

- Q3. Deputy Secretary Turk, in past years, almost all Federal departments and agencies have created new or expanded positions for Chief Information Officers, Chief Data Officers, or Chief Analytics Officers. In fact, the Department of Energy currently has a Chief Data Officer, reporting to the Chief Information Officer. Recently, some in Congress have called for the creation of yet another position – Chief AI Officers. Does the Department of Energy need additional bureaucracy and organizational bloat to effectively manage its own AI development or do you believe the Department has the organizational capacity and proven technical expertise already in place?
- A3. The Department of Energy needs to address two very important related but distinct goals to advance progress in AI. The first is our agency's internal usage of AI for activities such as operations, data management, or productivity in support of the DOE workforce. Any AI systems fully deployed for these purposes must be trustworthy and secure. The second is DOE's role in promoting research and development advances in AI in support of DOE's missions in science, energy, and security. DOE is committed to effectively and efficiently utilizing our staff and resources to ensure that we achieve both goals.
- Q4. Deputy Secretary Turk, we are in a state of technological and geostrategic competition with the Chinese Communist Party. How is American AI research and development competing against Chinese AI research and development? What is necessary to maintain American A.I. leadership?

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

- A4. For continued U.S. technological advantage in AI, the country needs to invest strategically while ensuring that these investments are underpinned by robust research security measures. With sustained investment, we will have world-class enabling infrastructure - the hardware, software, scientific data, and workforce - for large scale AI research and development. Thanks to support from Congress, we have already started making investments that will advance our understanding of trustworthy AI. In the recently published report, AI for Science, Energy, and Security, our National Laboratory experts have identified key areas where AI investments could be transformative in promoting innovation and advancements in technology while safeguarding our national security interests. This report serves as a roadmap on how future investments, along with leveraging the Department's existing infrastructure, can help maintain American leadership in AI.

Global competition in AI requires a transformative effort, involving whole-of-government action, mission-driven public-private partnerships, and collaboration with academia and non-governmental organizations. We also need to work with allies and partners, and we are actively working to develop and leverage those strategic partnerships. Throughout, DOE is committed to ensuring robust research security measures to minimize the risk of improper transmission of technologies and research.

- Q5. Deputy Secretary Turk, private firms are leading the charge in funding AI research. What role do you think the Department should play in funding research and why are you best positioned to lead AI funding beyond any other part of the Federal government?
- A5. While to date U.S. industry has had an outsized role in the development of certain AI technologies, industry alone cannot fully leverage AI in the national or public interest, nor comprehensively mitigate the risks associated with AI. Given the nation-state-scale investments happening outside of our borders, our nation requires unprecedented industry-government partnerships to maintain global leadership. Industry alone cannot be fully aware of the relevant risks and threats; much of that information falls within the purview of our Intelligence Community and our national security enterprise.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

Industry investments are also driven by market dynamics and the needs of their customers. The government has a unique role to play in developing the kind of unique models that can only be trained on supercomputers, such as models of molecular processes to unlock scalable low-defect additive manufacturing and models of the dynamics of the entire power grid. The government also needs access to classified models that ensure next-generation capability to manage threats to our national security, from space awareness to biodefense, nonproliferation, and nuclear deterrence.

DOE's existing infrastructure is a springboard for U.S. AI innovation:

- **World-leading 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 the most AI capable.^a
- **Advanced software:** DOE has created a wealth of science and engineering algorithms that can run on the most advanced supercomputers and is developing the world's first capable exascale software ecosystem that will drive breakthroughs in critical areas as varied as cancer research, energy production, and computational weapons applications.
- **Leading producer of both unclassified and classified scientific data:** DOE generates tremendous volumes of high-quality data across our network of 34 national user facilities around the country, as well as through industry partnerships and other research and development activities.
- **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.

^a TOP500 List – November 2023 <https://www.top500.org/lists/top500/list/2023/11/> (Accessed: January 5, 2024)

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

- Q6. Deputy Secretary Turk, it is well established that industrial and R&D espionage is a core practice of the Chinese Communist Party. In order to safeguard American innovation, and promote technological development in a democratic society, how is the US – and, specifically the Department of Energy - protecting and defending US IP?
- A6. DOE takes this issue extremely seriously and takes a risk-based, eyes wide open approach to protecting one of our nation's most valuable assets, our intellectual property (IP). Accordingly, DOE implemented a comprehensive and rigorous approach to research, technology, and economic security (RTES) as summarized below.

Intellectual Property Developed with DOE Funding

The Department takes its stewardship of taxpayer funded technologies and facilities extremely seriously. Like our groundbreaking scientific and technological solutions, protecting taxpayer funded intellectual property (IP) is, and has always been, part of DOE's DNA. Now under increasing threat of theft and misappropriation in the current hypercompetitive global environment, safeguarding DOE's and our nation's IP assets is indispensable to U.S. technological competitiveness and leadership. Risk-based IP protections for transformative scientific breakthroughs will help maximize our nation's competitive advantages, establish secure and resilient domestic supply chains, and continue to make the United States the most attractive destination for investment in new energy technologies which boost our energy security and independence.

DOE continues to adapt and evolve our IP safeguards as technologies and their associated risks change. The due diligence and vetting efforts spearheaded by the DOE Office of Research, Technology and Economic Security (RTES Office) and the continued stewardship of the Science and Technology Risk Matrix ensure that IP considerations will continue to be a key factor in risk management decisions across the DOE complex. In addition, after a comprehensive internal review of the IP licensing practices and procedures at our National Laboratories, the Department is currently working closely with our laboratory contractors to apply targeted risk mitigations and monitoring standards, including enhanced DOE oversight, to ensure that licenses to IP owned by our

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

National Laboratory contractors by law benefit the U.S. economy and taxpayers and protect U.S. economic and national security interests. DOE is also in the process of leveraging new authority under the Bipartisan Infrastructure Law to give our R&D partners additional data protection tools to better enable commercialization and help safeguard against potential misappropriation.

In addition, the Department remains fully committed to ensuring that innovation funded in America stays in America. In fact, DOE took administrative action in 2021 to go beyond minimum statutory obligations to require that new breakthrough science and energy technologies funded by the Department are manufactured here in America. This policy provides a strong signal that DOE is committed to ensuring that all technologies funded by the Department are manufactured in America by U.S. industry and labor whenever commercially feasible. Using DOE policy as a blueprint, in July, President Biden signed Executive Order 14104 formalizing the Administration's "Invent it Here, Make it Here" policy to ensure that the President's historic R&D investments in America benefit American workers, communities, and supply chain resilience. We are pleased to be a part of the Administration's initiative to support domestic manufacturing of technologies that are invented using DOE research funding.

DOE Disclosures and Foreign Talent Policies

Prior the passage of the CHIPS and Science Act, DOE took action to implement a similar prohibition regarding foreign talent programs sponsored countries of risk. DOE issued the DOE Order 486.1 "Department of Energy Foreign Government Talent Recruitment Programs" in June 2019, which is applicable to DOE employees, DOE National Laboratories, and other categories of DOE contractors. DOE updated the DOE Order in September 2020 to also include a restriction related to other foreign government sponsored or affiliated activities.

In 2022, DOE implemented current and pending support disclosure requirements for grants and cooperative agreements, which requires researchers to identify all involvement

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

with foreign talent recruitment programs, in addition to disclosing all resources made available to an individual in support of and/or related to all of his/her research efforts.

In 2022, DOE took action to prohibit members of a foreign talent recruitment program sponsored by a country of risk from participation in a BIL/IRA funded project or serving as a merit reviewer for a BIL/IRA funding opportunity announcement.

Due Diligence for Financial Assistance, Prizes and Loans

As part of DOE's effort, the Secretary established the RTES Office, which supports DOE program offices through: (1) pre-selection due diligence reviews of applications; (2) identification of appropriate safeguards (e.g. access controls for IP and other non-public information) in award terms; and (3) support throughout the life of a project to assess potential new risks of undue foreign influence that may arise (e.g., as new project partners are added or there are ownership changes to existing partners). The RTES Office falls under the Office of Foreign Investment & National Security, and Technology Collaboration, within the Office of International Affairs.

It is important to note, however, that while the RTES Office leads and coordinates DOE's research security efforts, it draws on, trains, and helps spread best practices among the broader RTES expertise and resources that are located throughout the Department. To ensure that RTES risks are considered early in the competitive process and throughout the life of a DOE-supported project, DOE instituted an enhanced due diligence process that leverages DOE's existing processes and incorporates best practices from other agencies. The enhanced due diligence process is a risk-based approach that relies on both open-source and classified sources, as appropriate. DOE integrates RTES reviews at three major points: (1) before a solicitation is released (to ensure the appropriate RTES requirements are included); (2) review of applications before selection; and (3) during the project implementation.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

Research Security at National Labs

DOE has developed, in partnership with the national laboratories, a Science and Technology (S&T) Risk Matrix to protect emerging research and technologies.

The S&T Risk Matrix highlights areas of emerging research and technologies and provides guidance to address potential concern associated with economic and/or international competitiveness that does not overlap or supersede existing controls associated with national security or export controls.

The S&T Risk Matrix uses a Red/Yellow/Green categorization format to quantify the risk associated with a given topic and the resulting level of controls that are required, with red assessed as highest area of risk.

The S&T Risk Matrix applies only to the national laboratories and for international transactions that include country of concern foreign national access requests to the laboratories, travel to countries of risk on restricted topics and country of risk engagement requests with the national laboratories.

For technologies or information determined by DOE in the S&T Risk Matrix to be less sensitive and not restricted, where DOE believes the collaboration will result in a net gain to DOE and the U.S. scientific enterprise, DOE promotes collaboration with nationals and entities, including countries such as China. As this Committee very well knows, countries of concern are limited to China, Russia, Iran and North Korea.

Additionally, in 2019, the Department established a policy prohibiting DOE personnel, to include laboratory M&O contractors, from participating in Talent Recruitment Programs sponsored by countries of concern.

In 2020, that policy was expanded to include a restriction of Other Foreign Government Sponsored or Affiliated Activities sponsored by countries of concern. Participation in these activities must be approved by the Secretary of Energy. The scope of covered

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

activities includes the following: employment, in-kind contributions or promises of future employment in the form of grants, awards, funding, scholarships, and appointments.

The purpose of these policies is to specifically address potential Conflict of Interest (COI) and Conflict of Commitment (COC) that China and other countries use to co-opt DOE researchers and thereby undermine U.S. national and economic security. We work to continually evaluate their effectiveness and improve procedures in order to maximize security for sensitive laboratory information while minimizing negative impacts to critical collaborative efforts among the global scientific community. We also seek to ensure that the administrative burden of these policies and programs is manageable and that our policies do not fuel xenophobia or prejudices in any way.

- Q7. Deputy Secretary Turk, major commercial providers of Large Language Models (LLMs) such as OpenAI and Anthropic admit to some level of human level censoring or "guidance" of model output. Do you agree with this censorship? Do you believe in conducting research and experiments using uncensored LLMs?
- A7. Large Language Models (LLMs) take many forms, and human judgment is always involved in development, design, and deployment of LLMs and related software systems. Because the Department conducts research on artificial intelligence as part of its scientific, energy, and security missions, we need to have an agile toolkit for testing and evaluating AI models and managing their attendant risks. Part of this research includes understanding bias and other elements of trustworthy and safe AI, and the ability to systematically test these LLMs.
- Q8. Deputy Secretary Turk, the Biden Administration's Office of Science and Technology Policy has released a so-called "Blueprint For an AI Bill of Rights" that covers the areas of "Safe and Effective Systems", "Algorithmic Discrimination Protections", "Data Privacy", "Notice and Explanation", and "Human Alternatives, Consideration, and Fallback." Do you believe this "Blueprint" will lead to the creation of large scale regulation of AI within the federal government?
- A8. The administration's Blueprint for an AI Bill of Rights is a set of five principles and associated practices released to help guide the design, use, and deployment of automated

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

systems to protect the rights of the American public in the age of AI. The principles, developed through consultation with the American public, are a blueprint for building and deploying automated systems that are aligned with democratic values and protect civil rights, civil liberties, and privacy.

In addition to releasing the Blueprint for an AI Bill of Rights, the Administration secured voluntary commitments from leading AI companies to manage risks posed by AI, issued an Executive Order, and is pursuing bipartisan legislation to keep Americans safe.

DOE and its National Laboratories are ready to provide technical expertise to inform regulatory discussions; however, DOE's primary role will be to remain on the AI frontier, driving AI innovation for science, energy, and security.

- Q9. Deputy Secretary Turk, in the Office of Science and Technology Policy's "Blueprint For an AI Bill of Rights" in the section entitled "Relationship to Existing Law and Policy" it states, *"Some of these protections are already required by the U.S. Constitution or implemented under existing U.S. laws. For example, government surveillance, and data search and seizure are subject to legal requirements and judicial oversight."* What, then, is the case for creating new regulation or legislation specifically for AI that is already covered by existing laws? What do you believe is not already covered by existing law?
- A9. We refer questions on the intent of the Blueprint For an AI Bill of Rights to OSTP, the primary author of the document. The recent AI Executive Order lays the groundwork for development of regulations, but these responsibilities are the remit of other agencies. If needed, DOE will provide technical input to other agencies which may inform regulations, such as in the case of determining the technical conditions for models and computing clusters for dual-use foundation models that are subject to reporting requirements, but developing the legal analysis for the need and scope of those regulations would remain with those agencies.
- Q10. Deputy Secretary Turk, in your opinion, what are the fundamental duties of the developers of a new AI system to current and future users? Are those duties different from those of current non-AI software developers?

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy’s Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

- A10. The fundamental duties of developers of AI systems include creating systems that are safe and effective, protect from algorithmic discrimination, have built-in protections for data privacy, provide notice and explanation, and provide options for human alternatives, consideration, and fallback^a not infringing on individuals’ and communities’ exercise of civil rights, civil liberties, privacy, equal opportunities, and access to critical resources or services, including a focus on equity. The use of massive amounts of data affords new opportunities and challenges for computing, and developers must bear in mind the potential impacts from collection and analysis of that data.
- Q11. Deputy Secretary Turk, in his testimony before Congress, OpenAI’s CEO Sam Altman stated, “the U.S. government should consider a combination of licensing or registration requirements for development and release of AI models above a crucial threshold of capabilities.” Do you agree with this sentiment (i.e. that there would be a threshold level requirement to apply for license or to register a new A.I. system)?
- A11. DOE takes the development of safe and secure advanced AI models seriously, and regulation – including licensing and registration requirements - needs to build on deep technical knowledge of the benefits and risks of AI. Regulation must also take into account an understanding of this rapidly evolving technology.

To move towards safe, secure, and transparent development of AI technology, the Biden-Harris Administration has secured voluntary commitments from leading AI companies on a set of principles including internal and external security testing of their AI systems before their release. The companies also committed to publicly reporting their AI systems’ capabilities, limitations, and areas of appropriate and inappropriate use; the disclosures are to cover both security risks and societal risks, such as effects on fairness and bias. On October 30, 2023, the Administration also issued an Executive Order on AI which will also focus on managing risks, keeping Americans safe and maximizing the benefits of this technology.

^a Blueprint for an AI Bill of Rights (2022) <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

- Q12. Deputy Secretary Turk, the Department of Energy has a wealth of highly educated, skilled, and experienced technical experts and leading researchers. How will the Department work to meet future workforce needs as they relate to AI?
- A12. DOE invests in the preparation of a sustained talent pool to meet future AI workforce needs. This includes support for thousands of young researchers through research grants to universities and dedicated STEM workforce training opportunities at DOE national laboratories in AI-focused or AI-enabled areas. DOE will need employees with the skills to ensure system trustworthiness and a culture of responsible practice. This will involve a workforce that knows how to deploy and use AI systems safely, overcome “automation bias,” evaluate whether a non-deterministic system meets the needs of its intended users, and set organizational policies for information-sharing about system and data characteristics and flaws.

Within the Office of Science (SC), the Early Career Research Program bolsters the nation’s scientific workforce by supporting exceptional researchers at the outset of their careers, when many scientists do their most formative work. The Computational Science Graduate Fellowship (CSGF), jointly funded by the DOE SC and the National Nuclear Security Administration, affords graduate students the support and freedom to pursue research and training in computational science areas including AI. The CSGF participants are required to do at least one practicum (research experience) at a DOE national laboratory during their fellowship. The practicum is a unique opportunity for DOE CSGF fellows to work with some of the most respected scientists in the world. This experience offers the fellows insight into how their scientific interests can translate to research areas important to the nation. Besides computational science, all SC’s science programs offices support graduate students and postdoctoral researchers in AI-related areas.

In addition to research grants, SC supports dedicated STEM workforce training programs, including undergraduate internships, graduate thesis research, and visiting faculty appointments, through the Office of Workforce Development for Teachers and Scientists. The training programs leverage the world class scientific expertise, unique

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

user facilities and capabilities, and resources at DOE national laboratories to provide students and educators the opportunities and mentorship for discovery learning and authentic research experiences in DOE science and technology areas, including AI. The Oak Ridge National Laboratory's Pathways to Computing Internship Program (PCIP) is a summer experience that provides undergraduate students with learning opportunities in computer science, computational science, and mathematics. SC also launched the Reaching a New Energy Sciences Workforce initiative and the Funding for Accelerated, Inclusive Research program, which together build research training at institutions not well represented in the science and technology ecosystem.

The NNSA funds several university consortia to support nuclear security objectives and provide a conduit to migrate top talent toward technical applications in nuclear security and the nation's national laboratories. For example, the Consortium for Enabling Technologies & Innovation works on developing and refining technologies supporting the nonproliferation mission to detect and characterize the production of nuclear materials, including basic research in artificial intelligence.

- Q13. Deputy Secretary Turk, please provide insights into the Department of Energy's current and future efforts to harness the potential of AI in optimizing energy exploration processes, enhancing energy capture technologies, and improving overall energy efficiency? Additionally, any information regarding collaborations with industry partners or research institutions in this regard would be greatly appreciated.
- A13. DOE's current and future efforts to harness the potential of AI are founded on and grow from decades of investments in applied mathematics, computer science, computational science, and next generation computing facilities. They span activities across the Department and our laboratories, including but not limited to our Office of Science (SC), our Energy Earthshots™, and our Office of Fossil Energy and Carbon Management (FECM).

The Frontier high performance computer at the DOE Office of Science-supported Oak Ridge National Laboratory Leadership Computing Facility (OLCF) is rated highest in the

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

world for its AI capability (nearly 10 ExaOps of mixed precision performance) and is a resource for the whole research community, including industrial users. OLCF also provides open access to the pre-exascale Summit system, ranked fifth for AI capabilities (nearly 1.4 ExaOps of mixed precision performance). Both Frontier and Summit offer a secure container, CITADEL, certified for use with sensitive data and codes including private health data and export control codes. OLCF is developing a virtual supercomputer—a digital twin to the Frontier system—that can be used to simulate and optimize the scheduling, cooling, energy consumption, asset life, and even user behavior of the Frontier supercomputer itself. The Frontier digital twin uses a combination of complex simulations, AI/Machine Learning (ML), and telemetry data to make autonomous decisions in real-time that realize value. Through its thermal cooling model and analysis, the digital twin has already helped OLCF gain better understanding of the energy conversion overhead and new insights on ways for improving energy usage and operational efficiency.

The Argonne National Laboratory Leadership Computing Facility (ALCF) provides an AI testbed resource for the community, featuring expert support and customized hardware from industry partners Cerebras, Samba Nova, Graphcore, and Groq. It also has plans to add a Grace Hopper testbed in FY 2024. The ALCF also offers access to the Polaris and Theta testbeds, with NVIDIA's Ampere Graphical Processing Units (GPUs). Community access to the Aurora Exascale system, with Intel's new GPUs, is planned for FY 2024. These are just a few examples of the types of deep collaborations between our national labs and industry partners.

DOE's Energy Earthshots aim to accelerate breakthroughs of more abundant, affordable, and reliable clean energy solutions within the decade. AI is a key tool for achieving these ambitious goals, including the Carbon Negative Shot, which aims to remove CO₂ from the atmosphere and durably store it at meaningful scales for less than \$100/net metric ton of CO₂-equivalent within a decade.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

FECM has over 130 current projects where AI is a key technology enabler. Approximately 2/3 of the AI applications fall into one of three categories: optimizing energy exploration processes, enhancing energy capture technologies, and improving overall energy efficiency; the remainder of the projects focus on improving productivity through data reduction. AI use cases include screening materials for carbon capture, detecting well- and facility-integrity issues, and forecasting offshore landslide risks and marine geohazards.

Besides the national labs, FECM has projects with AI as a component-leveraged collaboration with over 30 universities, research institutes and businesses acting as prime performers.

Information on optimizing energy exploration processes

Fossil Energy and Carbon Management's Methane Mitigation Technologies program has partnered with Pacific Northwest National Laboratory to use AI/ML in the development of computational tools designed to advance the state of the art in natural gas pipeline infrastructure integrity management. Leveraging machine learning and predictive data analytics offers new opportunities to develop methods for forecasting when and where in that network pipeline integrity and reliability may be compromised. Collectively, this suite of computational tools will be used by industry to cost effectively and accurately characterize the current health of pipelines, saving time and enhancing worker safety.

By engaging the expertise in DOE's national lab complex, FECM is also working on using AI/ML to explore and characterize new mineral deposits, helping accelerate the time it takes for industry to identify mineral reserves and produce new critical mineral resources.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

Enhancing energy capture technologies

FECM's Undocumented Orphan Wells program leverages the expertise of five National Labs to develop technologies, techniques, and best practices to locate and characterize undocumented orphan wells under the Bipartisan Infrastructure Law. As part of this effort, AI technology is being used to extract digital data from scanned well documents, extract well locations from historic maps and photos, and identify wells in multi-modal field data sets. Identifying orphan wells will help Federal agencies tackle legacy pollution, reduce greenhouse gas emissions, create good-paying union jobs, and benefit disproportionately impacted communities.

Improving overall energy efficiency

FECM's Natural Gas Decarbonization and Hydrogen Technologies program's Subsurface Hydrogen Assessment, Storage, and Technology Acceleration project leverages capabilities and demonstrated expertise across national laboratories to determine the viability, safety, and reliability of storing pure hydrogen or hydrogen-natural gas blends in subsurface environments. To identify prospective underground hydrogen storage fields, AI techniques are increasingly employed to significantly reduce costs associated with geophysical data and well log interpretation while improving accuracy and decreasing run times.

- Q14. Deputy Secretary Turk, could you please share insights into the Department of Energy's current and future efforts to foster AI education and research in collaboration with universities? Additionally, I am interested in understanding any programs or incentives in place to attract AI professionals to contribute their expertise to the Department of Energy's mission.
- A14. DOE supports AI scientists, engineers, and technicians at National Labs through laboratory work authorizations consistent with DOE's management and operating contracts to contribute their expertise to DOE's mission. Furthermore, DOE provides best-in-class, hands-on research and technical training experience at DOE labs (such as internships or visiting appointments) to sustain a diverse STEM talent pool ranging from

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

K-12, through undergraduate and graduate, to postdoctoral levels to ensure an AI ready workforce tomorrow. Additionally, DOE's Office of Science supports the Visiting Faculty Program (VFP) through its Office of Workforce Development for Teachers and Scientists. The VFP provides appointments of research collaboration with DOE national laboratories to faculty members from U.S. institutions of higher education historically underrepresented in the STEM research community, including all HBCUs. The VFP program has two tracks: research competitiveness and STEM teaching initiative. Through the research track, the VFP contributes to building research capacity of the participating faculty's home institution, and through the teaching track, faculty members bring back to their home institutions new research ideas and knowledge/skills to invigorate STEM curriculum for teaching and learning at home institutions in critical areas such as AI.

NNSA also provides several resources which are available for AI training and scientific simulation. These resources include the Crossroads and Sierra large-scale classified High Performance Computing (HPC) platforms. In 2024, NNSA will deploy the El-Capitan exascale computing platform, which is expected to be one of the largest computational resources in the world and will provide significant AI training capabilities.

NNSA also operates several University partnership programs, including the Defense Nuclear Nonproliferation (DNN) R&D University Consortia (outlined earlier) and the Defense Programs Predictive Science Academic Alliance Program, which aims to advance science-based modeling and simulation technologies in U.S. academia. These programs typically pair university professors and students with leading scientists at the DOE national laboratories. AI is already an important component of these programs and will expand in the future. These programs allow NNSA to develop AI professionals who can work not only with leading AI models but also use them to address the complex science and engineering challenges which are required for stockpile stewardship and other national security missions.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

The Office of Cybersecurity, Energy Security, and Emergency Response (CESER) will continue to explore ways to incorporate AI education and research, as it pertains to the energy sector, specifically towards cyber and physical security. In addition to the incorporation of a baseline understanding of how AI could influence the sector, CESER will continue to incorporate AI into agendas with the energy sector leadership and coordinating councils.

- Q15. Deputy Secretary Turk, please provide details on the Department of Energy's initiatives and strategies aimed at ensuring the security and integrity of large language models. Specifically, I am interested in any ongoing efforts or collaborations aimed at evaluating and enhancing Department of Energy cybersecurity assurance and so called "red-teaming" practices.
- A15. DOE recognizes the importance of managing risks associated with AI models, systems, and data in light of modern AI capabilities, and is currently working with its national laboratories to develop appropriate guidance that addresses these concerns while upholding our commitments to research transparency and equitable public access. These efforts will build upon the recent update of the Department's Science and Technology Risk Matrix, which is used to manage risks associated with critical and emerging research and technologies that require protection.

NNSA's DNN is working with its counterparts at the Departments of Commerce, Defense and State to develop export controls on critical and emerging technologies including AI/ML. DNN is working to make sure that technical experts from the DOE/NNSA national laboratories are able to contribute their technical expertise to the regulatory development process.

In addition, NNSA has decades of experience in developing and applying verification and validation techniques to our core modeling and simulation activities. Many of these techniques help to quantify and describe levels of accuracy and scientific confidence. Research staff at the DOE national laboratories are already engaged in research to apply

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: Recent Advances in Artificial Intelligence and The
Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging
Technologies
Questions for the Record Submitted to the Honorable David M. Turk

these methods or to develop complementary approaches that can provide us with similar rigorous frameworks to quantify the accuracy and integrity of machine learning models.

On the specific topic of red teaming, NNSA is already engaging with leading artificial intelligence companies in the United States as well as subject matter experts at the DOE national laboratories. Best practices and methods in this area are emerging and will continue to evolve over time as both NNSA and industry deepen their understanding of the technology and how the models may be evaluated for issues such as data inaccuracy, security weaknesses, exposure of sensitive data and the provision of mis- or dis-information. Additionally, NNSA has several programs underway to develop AI capabilities for nuclear proliferation detection and safeguards. The test and evaluation methods developed within these programs are often directly applicable or adaptable to use in red teaming of AI, and NNSA is evaluating how to leverage these advances for development of future red teaming capabilities.

U.S. Senate Committee on Energy and Natural Resources
 September 7, 2023 Hearing: *Recent Advances in Artificial Intelligence and The Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging Technologies*
 Questions for the Record Submitted to Dr. Rick L. Stevens

Questions from Ranking Member John Barrasso

Question 1: Please describe in detail how DOE National Laboratories promulgate training data to train their proprietary models.

How does DOE ensure training data for AI models is selected without bias and without favorability as a means to elicit a given researcher's favored outputs?

While the exact practices may vary between laboratories, there are overarching principles and community practices that guide the handling, usage, and dissemination of training data and the development of AI models within the labs.

Handling and Promulgation of Training Data: Typically, the DOE National Laboratories may employ a combination of publicly available datasets, partnership-derived datasets, and proprietary datasets that are developed in-house or acquired through collaborations. Some datasets are derived from experiments and others may be derived from large-scale computer simulation depending on the target application. It is important that the labs ensure that data is disseminated in a way that is secure, compliant with relevant policies and regulations, and adheres to ethical research principles. When training models, sharing, or releasing datasets, it is common practice to anonymize or aggregate data to protect sensitive information and individual privacy.

Mitigation of Bias and Ensuring Objectivity: DOE National Laboratories and the wider AI research community are increasingly focused on addressing biases in AI models and training data. Here are some of the approaches that are used at the laboratories.

- **Data Preprocessing and Examination:**
 - The labs implement rigorous preprocessing and examination procedures to identify and mitigate biases in the datasets. This may involve analyzing data distributions, removing outliers, and balancing class distributions. Data augmentation methods are often used.
 - They also perform comprehensive audits of datasets to ensure they are representative and do not contain inadvertent biases.
- **Diversity in Data Collection:**
 - Efforts are made to ensure diversity and inclusivity in data collection processes, and, where appropriate, consider factors like geographic location, demographic attributes, etc.
 - Multi-disciplinary teams including domain experts, ethicists, and data scientists collaborate to evaluate and ensure the diversity and representativeness of datasets.
- **Bias Detection and Mitigation Techniques:**
 - Advanced techniques like adversarial training, fairness-aware modeling, and sensitivity analysis are used to detect and reduce biases in the AI models.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: *Recent Advances in Artificial Intelligence and The Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging Technologies*
Questions for the Record Submitted to Dr. Rick L. Stevens

- Fairness metrics are also applied to evaluate models and continually monitor models in deployment to assess and address any emerging biases.
- **Transparent and Reproducible Research:**
 - The labs adhere to principles of transparency and reproducibility. They share methodologies, and, when possible, code and datasets to allow peer review and independent verification of results.
 - They document any potential biases or limitations in the datasets and models and communicate them transparently in research publications and reports.
- **Ethical Guidelines and Oversight:**
 - Ethical guidelines and oversight mechanisms, including Institutional Review Boards (IRBs), guide the selection and use of data for some areas.
 - Researchers are trained in ethical AI principles, and ongoing dialogue on ethics and fairness in AI is encouraged within the scientific community.

Community Engagement and Collaboration: The DOE National Laboratories collaborate with academia, industry, and other research institutions, contributing to the broader AI research ecosystem. Engaging with diverse stakeholders allows for the cross-pollination of ideas and best practices, which helps develop models that are more robust, unbiased, and generalizable.

Feedback and Iteration: Feedback from peers, collaborators, and the wider research community is instrumental in refining models and addressing biases. The iterative nature of model development at the labs involves continuous refinement and improvement of models based on insights and feedback from diverse sources.

Summary: While specifics can vary based on the target problems, level of classification, etc., the DOE National Laboratories follow a rigorous, ethical, and collaborative approach in selecting and using training data for AI models, with robust measures in place to mitigate bias and ensure objectivity and fairness. Regular updates, dialogue on ethical AI principles, and community engagement further reinforce these practices, ensuring alignment with the evolving best practices in the AI community.

Question 2: What criteria must be met for a DOE AI model to be considered deployable for internal use and/or potential use by the general public?

For a DOE AI model to be considered deployable, several rigorous criteria typically need to be met. While specific requirements may vary depending on the application, the general criteria include the following areas:

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: *Recent Advances in Artificial Intelligence and The Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging Technologies*
Questions for the Record Submitted to Dr. Rick L. Stevens

Accuracy and Reliability: In addition to technical measures to assess accuracy and reliability, models that will be released externally will undergo peer review that is internal and/or external depending on the scenario.

- The model should have undergone extensive testing and validation to ensure accuracy and reliability in predictions or classifications.
- The model's performance metrics should be at an acceptable level.

Security and Privacy: Depending on the target problem there are several criteria to address related to security and privacy. An important issue is to understand if the model contains, or can generate, any information that should not be released.

- The model must comply with all relevant federal and departmental security policies and standards to protect sensitive and classified information.
- Privacy concerns, particularly those involving personally identifiable information (PII), must be addressed, and data should be handled in accordance with applicable privacy laws and regulations.

Ethical Considerations and Bias: Many DOE National Laboratory models are used in technical scenarios (e.g., generating code or making predictions of a scientific nature where bias has a different meaning), however, when models are being deployed for operational purposes or for use outside the laboratory settings, additional criteria are used such as:

- The model must be evaluated for fairness, accountability, transparency, and potential biases and should align with ethical AI guidelines and principles.
- The potential impacts of the AI model on individuals and communities should be thoroughly assessed and mitigated.

Usability and Accessibility: Like deploying software systems for broad range of applications in DOE National Laboratories, AI models need to be assessed for fitness of purpose and accessibility to relevant user communities.

- The model should be user-friendly and should be accessible to the intended user base, including people with disabilities.
- Clear documentation and user guidelines should be available to ensure proper usage.

Compliance with Legal and Regulatory Frameworks: Like release of publications or software, work products of the laboratories must follow any applicable legal and regulatory requirements. Similar review prior to publication is utilized at the DOE National Laboratories.

- The model must adhere to applicable laws, regulations, and guidelines, including federal acquisition regulations if applicable.
- Any intellectual property concerns should be addressed.

Scalability and Performance: Depending on the application, scalability and performance could be important metrics, including energy efficiency of the model. Some of these issues are also related to the hardware platform the model is targeting.

- The model should be scalable and should perform adequately under varied loads and conditions.

U.S. Senate Committee on Energy and Natural Resources
September 7, 2023 Hearing: *Recent Advances in Artificial Intelligence and The Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging Technologies*
Questions for the Record Submitted to Dr. Rick L. Stevens

- It should be optimized for efficient resource usage.

Robustness: It is difficult to anticipate all the ways in which a model might be used, however, understanding how a model handles novel inputs is important for some deployments.

- The model should be able to handle real-world data and conditions effectively and be robust to variations in input data.
- It should have mechanisms to handle errors gracefully.

Interoperability: Models are often deployed as part of an existing workflow or as a component in a complex system. In these cases, it is important that the model interoperate with existing systems in expected ways.

- The model should be compatible with existing systems and technologies and should follow established standards for interoperability.

Maintainability: Models need to be updated to stay current, and as training data changes or improves, every attempt is made to see that models can be maintained over the expected lifetime of the model.

- The model should be maintainable and should have support for updates and improvements.
- Adequate documentation of the code, architecture, and training data should be available to allow for future modifications and improvements.

Risk Management: A risk assessment is needed for some models that are deployed in high-consequence environments, including any public release of models.

- Potential risks, including unintended consequences and misuse, should be identified, and mitigated.
- A contingency plan should be in place for addressing any issues or failures post-deployment.

Transparency and Documentation: Enabling others to understand models and to reproduce them and their behavior is important in many applications and is an essential element of peer review.

- Clear documentation detailing the model's workings, limitations, usage guidelines, and other relevant information should be readily available.
- The development process, including data collection and model training, should be transparent and well-documented.

Meeting these criteria would generally allow a DOE AI model to be considered deployable for internal use and/or potential use by the public. However, the exact criteria and the process may vary depending on the specific application. DOE's processes and criteria are well aligned with best practices in the community.

QFR's for Senate Committee on Energy and Natural Resources Hearing on "recent advances in artificial intelligence and the Department of Energy's role in ensuring U.S. competitiveness and security in emerging technologies"

Anna B. Puglisi
Senior Fellow

Center for Security and Emerging Technology (CSET), Georgetown University
30 September 2023

Questions from Ranking Member John Barrasso

Question 1: You have a strong background in bio-security. There are numerous applications of artificial intelligence in fields of health and biology. What insights or concerns have you identified related to the role of artificial intelligence in these fields, especially as it relates to national security?

We are on the cusp of game-changing discoveries in biotechnology driven by advances in AI. These applications include identifying drug targets, image screening, and predictive modeling of proteins and nucleic acids. The use of AI in basic research promises to shorten research timelines, enable analysis that was previously impossible, and open new fields of research, given AI's ability to process the vast amounts of experimental health and environmental data generated by today's researchers and support an understanding of these data. The following areas are drivers of this change:

Bioinformatics

Bioinformatics can be described as using computation and statistics to understand biology, allowing scientists to better understand the function of genes and proteins, three dimensional shapes of proteins and nucleic acids, and the evolution of parts of the genome. AI takes this field to the next level by enabling more efficient data processing and analysis, expediting the translation of experimental science to real world applications. China has prioritized bioinformatics, fostering national champion BGI, as well as establishing key enabling infrastructure. Bioinformatics is inherently interdisciplinary in scope, comprised of engineering, statistical, biological, and other subdisciplines. As a way to enable this development, China is promoting "industrial clusters" to bridge these gaps and bring together different disciplines.

Synthetic biology

Described by the U.S. National Institutes of Health (NIH) as "a field of science that involves redesigning organisms for useful purposes by engineering them to have new abilities,"¹ synthetic biology offers new ways to harness nucleic acids for a wide range of applications. The use of AI to find ways to connect genotypes with phenotypes—basically understanding what genes do and what they code for—has implications for understanding human disease, genome manipulation, and designing life-saving therapies, not to mention increasing the probability of lab accidents, violating ethical boundaries, and creating new or enhancing existing biological weapons.

Gain of function research

Research that, purposefully or not has the effect of enhancing the virulence or transmissibility of pathogens has direct national security implications. While there are valid reasons for concern, there are also important questions this research can answer that help the biomedical sector prepare for future pandemics. The ability to better understand how pathogens and their hosts interact on the molecular level, and how proteins and other biomolecules function in the cell, will be enabled by AI, yielding potential implications for this line of research.

Agricultural biotechnology

Food security will likely become more of a national security issue as countries worldwide grapple with ways to feed their citizens. Better understanding of genomic factors that impact growth, disease resistance, and the nutritional value of plants and livestock has the potential to impact world hunger and to become a key economic driver. AI is already being used to manage fields for increased yields. Its use to study plant and animal genomics will affect our ability to grow resources for livestock and modify livestock in ways that facilitate ease of handling (e.g., hornless cows)—not to mention replacing them with plant-based substitutes.

Data privacy, data security, and population surveillanceⁱⁱ

While not a facet of biotech research itself, as more genomic and other biological information becomes available, AI's impact on our ability to store, analyze, and protect it is increasingly important. The US and like-minded countries will need to explore whether current procedures governing data privacy are sufficient, or if there are special considerations unique to genomic data. Key among these considerations will be how to maximize discovery while protecting this resource vis-à-vis other countries that do not play by the same rules for sharing and collaboration. It will be important to consider not only what is possible now, but what may become possible in the future. As the field matures, what is not necessarily alarming now—access to a wide range of genomic data—may provide an advantage to researchers who have it.

However, while it is important to understand what genes do, and why analysis of genomic data with AI holds a lot of promise, there are still many things about cell functions and genomic pathways we do not understand. It will take a better understanding of these aspects of biology to be able to implement all of the range of possibilities highlighted in the many studies and discussions of this technology.

Question 2: What restrictions does the Chinese government impose on American citizens conducting research in China? Are Chinese citizens subject to the same level of restrictions when conducting research in the United States?

We have not conducted a comprehensive examination of the differences in how China and the U.S. treats its visiting scholars and scientists. We agree that this would be an interesting study,

especially if it compares and contrasts those in academia, the DOE labs and companies. However, given our understanding of China's authoritarian system, and the openness of our own, the following are some areas that are likely different:

- Freedom of Movement: This would include the ability to visit specific facilities and also how much access U.S. scientists are given when visiting a university, research entity or State Key Lab.
- Access to the computer systems.
- Ability to freely and completely share data and scientific results

ⁱ <https://www.genome.gov/about-genomics/policy-issues/Synthetic-Biology>.

ⁱⁱ Here "population surveillance" means collecting DNA samples from humans, not genomic surveillance of pathogens to identify emerging diseases.



FAS@FAS.ORG
FAS.ORG

FEDERATION OF AMERICAN SCIENTISTS
1112 16TH STREET NW, SUITE 600
WASHINGTON, DC 20036

Recent Advances in Artificial Intelligence and the Department of Energy's Role in Ensuring U.S. Competitiveness and Security in Emerging Technologies

Statement For The Record

Chairman Manchin, Ranking Member Barrasso, and members of the Senate Energy and Natural Resources Committee. I appreciate the opportunity to submit this statement underpinning the Department of Energy's visions to shape our strategic investments in AI.

The Federation of American Scientists (FAS) is a catalytic, non-partisan, and nonprofit organization committed to using science and technology to benefit humanity by delivering on the promise of equitable and impactful policy. FAS believes that society benefits from a federal government that harnesses science, technology, and innovation to meet ambitious policy goals and deliver impact to the public.

I am the Associate Director for Emerging Technologies and National Security at FAS where I lead our work on emerging technologies' policy from the lens of our national security innovation base, as well as focusing on the strategic competition between the United States and the Chinese Communist Party. I wish to commend your work in bringing the Committee together to discuss the Department of Energy (DOE)'s role in ensuring U.S. competitiveness and security in emerging technologies. This hearing could not have come at a more opportune time.

In March, the Chinese Communist Party (CCP) held its yearly "two sessions" meeting—referring to the coming together of China's principal political bodies, the National People's Congress (NPC) and the National Committee of the Chinese People's Political Consultative Conference (CPPCC)—during which they not only confirmed Xi Jinping's third term as president but also introduced a set of new policies and government appointments. During this meeting, Xi emphasized the importance of self-reliance in science and technology as a strategic goal to combat Western influence. Meanwhile, the Central Committee revealed plans to restructure the Chinese government to better position China's national innovation system for driving advancements in both commercial and dual-purpose military-civilian technologies. This latest initiative underscores two decades of unwavering CCP commitment toward indigenous innovation, calibrated specifically to outflank its Western competitors like the United States. And it's getting results: a recent analysis by the Australian Strategic Policy Institute found that China

now leads in 37 out of 44 critical technology areas globally, while Chinese production of high-value patents in the global marketplace has increased by 400% over the past decade.

The Committee's hearing is exploring a question that is of vital national interest. The two proposals—creating an Office of Critical and Emerging Technology within the DOE and the Frontiers in Artificial Intelligence for Science, Security and Technology—could change this trajectory for the better.

First, the creation of an Office of Critical and Emerging Technology within the DOE. This office would enable a robust assessment of U.S. technological competitiveness and prepare us for emerging technology surprises conveying a potential threat to national security. This framework will refine our strategic direction, facilitate rapid threats-response coordination with interagency collaboration from entities like DoD, DNI and NSF amongst others, while advancing proactive countermeasure strategies.

The Office should serve as a hub for innovative practices across all 17 National Labs and 34 user facilities that the DOE stewards. The DOE labs and user facilities have expertise and capabilities that are important in national and international science policy challenges. This office should promote greater participation from our labs to better inform these discussions, thereby effectively fostering a diversity of perspectives within national science policy discourse and international forums, which is ever-critical given the ascending competition from nations including China and Russia in domains like AI, quantum computing, and biotechnology.

Secondly, the FASST initiative—Frontiers in Artificial Intelligence for Science, Security, and Technology—is another imperative. AI's transformative potential is undeniable but demands substantial improvement in fundamental aspects like explainability, trustworthiness, reliability, especially for mission-critical applications and privacy-sensitive issues.

The DOE, with its high-performance computing prowess, is uniquely positioned to deliver secure and dependable AI solutions for the challenging problems of the century. By leveraging DOE's world-leading exascale computing capabilities while working synergistically with key stakeholders from academia, industry, and interagency groups, we can unlock groundbreaking AI innovations.

Efforts must be made to accelerate integrated math and science R&D, particularly foundational AI research to develop secure, trustworthy techniques. Rigorous verification and validation

processes, guided by scientific validity, can vet new technologies for their societal implications before widespread deployment.

Moreover, expanding on foundational research in physics-informed AI could lead to better integration of AI models with our understanding of real-world phenomena. This involves cooperative research among diverse specialties, an endeavor DOE labs and associated universities are equipped for.

The proposed multi-billion-dollar annual program involving DOE Office of Science, National Nuclear Security Administration, and applied energy programs aims to leverage unique leadership capabilities in computing to create transformative AI hubs focused on solving grand challenge problems, innovate world-class AI technologies, and harness cutting-edge testbeds for developing energy-efficient AI hardware platforms in concert with US industry.

Adding to the testimony, I would like to emphasize the pivotal role the FASST initiative will play in the development of unique open and secure foundation models for discovery and national security. The objective is to harness unique and highly-curated datasets to foster advancements and ensure that the United States remains at the helm of science and technology.

The creation of uniquely crafted models, possible only through supercomputing, will offer unprecedented insights into complex processes like molecular dynamics crucial for additive manufacturing or power grid dynamics, leading to a more resilient energy infrastructure. Moreover, it's crucial for the DOE to develop classified models to manage threats to our national security, from maintaining space situational awareness to advancing biodefense, nuclear deterrence, and nonproliferation efforts. However, I would also urge caution as this could provide our adversaries with a single point of attack to extract classified data if they were to gain access to the frontier model trained on classified data.

We are observing an unprecedented deployment of large language models and other advanced AI models like AlphaFold 2, AlphaGo, amongst others, across the country. AI tools and foundational models developed by the DOE could test and validate these AI tools. This capability is imperative to ensuring AI models deployed meet safety and ethical standards that align with our societal values. Furthermore, it will allow DOE to assess risks posed by other AI models that are outside of U.S. regulatory jurisdictions.

In terms of tool and software development, FASST could develop common platforms for safe, trustworthy AI suitable for high-stake usage scenarios. This would involve crafting tools and

methodologies that enhance the trustworthiness and reliability of AI systems while preserving privacy. It also involves an acute focus on cybersecurity, establishing classified platforms capable of evaluating potential adversarial AI systems.

The harnessing of both classified and unclassified scientific datasets will be instrumental in this endeavor. By transforming DOE's leading-edge facilities into a nationwide integrated research infrastructure, we will cultivate a common platform for training and evaluation, thereby deriving valuable findings from the world's largest volumes of scientific data.

Furthermore, FASST will be instrumental in bolstering state-of-the-art production capabilities for our nuclear stockpile by advancing the state-of-the-art in foundation models to rapidly validate AI technologies addressing emerging nuclear security missions. In addition, FASST's aims to develop new foundation models for unique types of data such as seismic and electromagnetic are worthy of support as these areas where current capabilities are lacking.

Through these concerted efforts, we aim to combine the strides in AI innovation with critical missions in science, security, and technology—encompassing scientific discovery, energy sustainability, and national security. We will continue to boldly ride the tidal wave of AI evolution while ensuring that we stay ahead of possible detriments that could compromise our nation's security and leadership in technology.

Eventually, the transformation of DOE facilities into a nationwide integrated research infrastructure can stimulate advanced AI research deployment across sectors, enhance resource utility, drive unprecedented growth potential, and reinforce U.S.'s techno-economic leadership.

In conclusion, championing these proposed provisions underscores the urgent need for research, development, and deployment to ensure our ongoing global competitiveness within the critical emerging technology fields. Proactive investments today promise substantial strategic dividends for our nation's future by maintaining its vital role in technological innovation while robustly addressing potential risks tied to these technological breakthroughs. At the same time, we must proceed with caution as our adversaries try to gain access to our classified information every hour of every day. Creating frontier models with classified information could provide significant benefits to our national security apparatus, yet at the same time, it could also provide our adversaries an easier path to gain access to our secrets, hence we must do it in a way that ensures our systems are safe, secure, and reliable.



FAS@FAS.ORG
FAS.ORG

FEDERATION OF AMERICAN SCIENTISTS
1112 16TH STREET NW, SUITE 600
WASHINGTON, DC 20036

In the end, this is not just about maintaining a competitive edge; this is about national security, about establishing ethical guidelines for technology usage; it's about mission-critical deployments where failure is unimaginable, about enhancing global standings through technological supremacy.

We believe this strategic investment into critical and emerging technologies will empower our nation to confront 21st-century challenges with solutions that are timely, scientifically rigorous, and security-enhancing. We express our unwavering support towards these provisions and encourage their decisive endorsement.

Thank you for considering our views on these pressing topics.

If you have any questions, please reach out to me at dkaushik@fas.org.

Divyansh Kaushik
Associate Director for Emerging Technologies and National Security
Federation of American Scientists