Dr. Shaun Gleason
Director, Science-Security Initiative Integration
Oak Ridge National Laboratory

Testimony of Dr. Shaun Gleason
Director, Science-Security Initiative Integration
Oak Ridge National Laboratory
Before the
U.S. Senate Committee on Energy and Natural Resources
September 12, 2024

Hearing on "Department of Energy's Leadership in the Next Generation of Advanced Computing Research, Application, and Security"

Chairman Manchin, Ranking Member Barrasso, and Members of the Committee: Thank you for the opportunity to speak with you today. My name is Shaun Gleason. I am the Director of Science-Security Initiative Integration at the U.S. Department of Energy's (DOE's) Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. I serve as a liaison between the open science and national security mission communities at ORNL. I am specifically focused on advancing emerging technologies such as artificial intelligence (AI), quantum science and technology, and advanced computing across the diverse mission areas of ORNL. I have been at ORNL for 35 years, and my research background is in electrical engineering with a focus on data processing, machine learning, and advanced computing platforms. I have previously served as the interim associate laboratory director for Computing and Computational Sciences and as the director of two research divisions at ORNL for which I was responsible for leading science and engineering capabilities that include quantum, AI, advanced computing, and cybersecurity for critical infrastructure. One of my director roles was entirely focused on cybersecurity for the national security mission and included sponsors such as DOE, the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Intelligence Community (IC). Finally, I am an entrepreneur who founded a startup company that successfully transitioned a medical imaging technology to the market.

As an introduction to my testimony, I am not here to provide opinions on legislation or policy but rather am here to share my technical expertise relevant to the subject of this hearing and how the DOE national labs, and ORNL in particular, provide national leadership. The views I present to you are my own and have been formed by my career as a researcher, engineer, entrepreneur, and technical leader. First, I will outline a few grand research challenges in AI, quantum, and cybersecurity that hopefully will motivate continued investment by Congress to advance the frontiers of science and innovation. Second, I will describe how cybersecurity, AI, and quantum science overlap and intersect and will present some research opportunities that exist at the crossroads of these technologies. Finally, I will emphasize how national labs are uniquely equipped

to push the boundaries of innovation and the importance of government, academic, and industry partnerships to accelerate science, innovation, technology transfer, and workforce development.

Grand Challenges

Some grand challenges require us to accelerate progress immediately to ensure continued U.S. leadership in the emerging technologies of quantum, cyber, and AI. Our economic, energy, and national security *require* that we continue to invest and innovate to solve the grand challenges across these three fields.

For AI, improving energy efficiency is an imperative, because many experts are predicting that energy use by AI-driven data centers will approach 10% of total U.S. energy demand by 2030. Other reports predict that AI will contribute to reduced energy needs, by enabling improvements such as more intelligent and efficient grid operation. ["AI and energy: Will AI help reduce emissions or increase demand? Here's what to know," World Economic Forum, July 2024, https://www.weforum.org/agenda/2024/07/generative-ai-energy-emissions/]**.** Either way, we must develop and deploy new hardware technologies such as quantum and neuromorphic AI coprocessors that have potential to solve AI computational problems with a much-reduced energy footprint. Energy efficiency is also critical for deploying AI "at the edge" for remote scientific experiments, grid control endpoints, and national security missions in areas where power sources are severely limited and/or unreliable. We need not only new hardware platforms but also new algorithms, software, and computational workflows that are more energy efficient. Another grand challenge in AI is the development of AI systems that are safe, secure from cyberattacks, and privacy-preserving (i.e., they preserve the privacy of sensitive data used to train the AI model). Addressing these and other grand challenges in AI will help the U.S. maintain leadership and strengthen our economic and national security.

For quantum, the potential positive impact is transformative, and the grand challenges are numerous. A primary challenge is the ability to create reliable, accessible, and affordable quantum devices such as quantum sensors and qubits for quantum computers. Creating such quantum devices requires basic R&D in physics and materials science, quantum engineering (the ability to turn a quantum material into a functional device), and, finally, manufacturability—so that these devices can be made reliably and affordably in large quantities. Solving this grand challenge will drive a second grand challenge of creating a large-scale (1,000+ qubit), fault-tolerant quantum computer that can solve real-world problems unsolvable by classical HPC systems. Examples include complex optimization problems in physics, chemistry, medicine, and logistics. Part of the grand challenge in quantum computing is the integration of classical high-performance computing (HPC) with quantum computers functioning as

coprocessors suited for quantum computation. Such hybrid classical-quantum computers must be easily programmed to solve important problems. A third grand challenge is quantum networking, which requires a new type of network that can reliably share quantum information across many different quantum devices (e.g., quantum computers, sensors, and photon sources) over long distances (hundreds of kilometers). Some refer to this as the "quantum internet." One key to solving this grand challenge is transduction, which is a method of reliably sharing different forms of quantum information with other devices on the quantum network.

Clearly, many grand challenges exist in the cybersecurity field. Cybersecurity is an "arms race" where every defensive move inspires an adversary's offensive move, and vice versa. The U.S. needs a revolutionary leap in AI-driven, adaptive cybersecurity to propel our cyber defenses out of reach of adversaries for both information technology (IT) and operational technology (OT) systems. OT systems are collections of components such as networks, computers, control systems, and sensors that provide supervisory control and data acquisition, process monitoring, and communication for critical infrastructures such as the electric grid, oil and natural gas systems, water treatment plants, and manufacturing systems. All of these systems provide essential and, often, lifesaving services. As an example, the U.S. electric grid is arguably the largest and most complex machine in the world, with approximately 60 million transformers of roughly 80,000 different types, 70,000 substations, and 5.5 million miles of distribution lines. [AI for Energy: Opportunities for a Modern Grid and Clean Energy Economy, DOE, April 2024, https://www.energy.gov/cet/articles/ai-energy] The OT system for the U.S. grid is a mix of both decades-old hardware and software components and brand new, "smart" Internet of Things devices, which increase the cyberattack surface of the electric grid. Compared with IT systems, there is little commonality in the operating systems and chip sets used across different OT systems manufacturers, which creates cybersecurity challenges. Regional variations across the U.S. such as the type of OT equipment used, mixes of distributed energy resources (nuclear, wind, solar, hydro, coal, etc.), population density and growth patterns, geographical differences, and weather extremes preclude the implementation of a uniform, nationwide approach to securing the grid. As such, solving this grand challenge requires regional partnerships and testbeds connected to a national cybersecurity coordination network.

Research Opportunities at the Intersection of Cybersecurity, AI, and Quantum

AI, cyber, and quantum are all broad research areas, and many advances are occurring rapidly within each individual field. Some of the most exciting areas for revolutionary innovations are where they intersect with one another.

For example, if we consider the fields of cybersecurity and AI, AI is being used to create dynamic, self-learning cyber defense tools that are equipped to adapt to rapidly changing cyberattacks against our nation's critical infrastructure. As an example, ORNL has built a Cyber Operations Research Range that employs HPC to help the U.S. Navy evaluate the effectiveness of commercially available AI-based cyber defense tools before they spend precious resources to acquire them. On the flip side, generative AI is being used to rapidly create volumes of never-before-seen instances of malware and ransomware, some of which can penetrate the best deployed cyber defense tools. To illustrate this point, ORNL demonstrated that AI could be used to modify existing malicious software (malware) so that it penetrated the latest commercially available AI-based cyber defense products approximately 80% of the time. This result was shared with vendors so they could work on improving their AI-based cyber defense tools. Finally, AI systems are uniquely vulnerable to specific cyberattacks, some of which manipulate the AI system into making decisions favorable to an adversary by "poisoning" the training dataset. An example of this would be creating data-rich websites that are automatically scraped for data used to train an AI model but that contain disinformation that biases the model. Other AI system attacks can enable an adversary to steal the sensitive data (e.g., personally identifiable information) used to train an AI model. A different type of attack attempts to fool the AI model into making a decision that is favorable to the adversary. As a simple example, an adversary could paint a special pattern on a military vehicle that fools an AI system into thinking it is a civilian vehicle. To combat these types of cyberattacks on AI systems, several of the DOE national labs have created organizations that are developing cybersecurity capabilities specifically for AI systems. These include ORNL's Center for AI Security Research (CAISER), Los Alamos National Laboratory's AI Risks and Threat Assessments Group (AIRTAG), Pacific Northwest National Laboratory's Center for AI, and Lawrence Livermore National Laboratory's (LLNL's) Resilient AI for National Security (RAINS) center. These organizations provide DOE-stewarded capabilities for the mission of other agencies outside of DOE, including DOD, DHS, and the IC.

Next, if we explore the intersection between the fields of AI and quantum science and technology, AI is being leveraged to accelerate discovery of new quantum materials, hypothesize new quantum computer designs, and generate new types of error correcting codes for quantum systems, all of which are needed to accelerate the development of the next generation of quantum computers. Conversely, quantum computers are being used to speed up machine learning training algorithms to enable deployment of fast, energy-efficient quantum coprocessors that can train and evaluate large AI models more efficiently than a classical HPC system. Quantum computers can also generate realistic simulated data that can be used to train data-hungry AI foundation models. For example, quantum computers can simulate molecular

interactions and generate vast amounts of training data to train AI models for new materials discovery. The discoveries being made at the intersection of the fields of AI and quantum are powerful, and the scientific community has just begun to scratch the surface.

At the intersection of the fields of quantum and cybersecurity, many academic and national lab research institutions are developing post-quantum cryptography methods that result in encryption methods that will be unbreakable by future quantum computers. These new approaches are critical because future quantum computers are predicted to be able to break the classical encryption methods used ubiquitously in our everyday lives, including those in our computers and smart phones. After eight years of collaboration among cryptography experts around the world, the National Institute of Standards and Technology just released the first three finalized post-quantum encryption standards. [https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards]

DOE's Unique Capabilities and Critical Partnerships

The final topic of my testimony covers the unique role that DOE plays and the importance of government, national laboratory, academic, and industry partnerships to accelerate innovation and technology transition across cybersecurity, AI, and quantum. The DOE national laboratory system is uniquely positioned to solve the grand challenges and advance science and innovation at the intersections of each of these emerging technologies. The national labs employ the largest multidisciplinary scientific workforce in the nation with approximately 70,000 employees. I often share with my family and professional colleagues that I can find a scientist at ORNL with deep technical expertise in every scientific area of interest including AI, cybersecurity, and quantum. This scientific depth is magnified when you consider the scientific talent across the entire DOE laboratory system. Therefore, the labs are uniquely equipped to innovate at the intersections of these three fields.

DOE's national laboratories are also home to large and extremely powerful experimental facilities that the labs make available to universities, industry, and other government agencies to conduct cutting-edge research. Thanks to investments by Congress through DOE's Office of Science and the National Nuclear Security Administration, these user facilities, stewarded by the national laboratory system, are the most unique and powerful experimental facilities in the U.S. They include exascale supercomputers—Frontier at ORNL, Aurora at Argonne National Laboratory (ANL), and, later this year, El Capitan at LLNL—that can be used to train and test the largest AI foundation models. The national lab system is also home to several of the world's most powerful tools for studying materials, including the Linac Coherent Light Source at SLAC National Accelerator Laboratory, Spallation Neutron Source at ORNL, National

Synchrotron Light Source-II at Brookhaven National Laboratory, and Advanced Photon Source at ANL, all of which can generate uniquely valuable data to train AI models targeted for new materials discovery. The combination of world-class talent, high-performance computation, and data-generating facilities enables DOE to foster revolutionary discoveries at the intersections of AI, cybersecurity, and quantum.

Another advantage of national lab engagement in development of these emerging technologies is that DOE and its national labs have policies, procedures, tools, and infrastructure that provide layers of security enabling both classified and unclassified research on sensitive, critical, and emerging technologies. We cannot maintain U.S. leadership in fields such as AI, quantum, and cybersecurity without training our domestic workforce and leveraging the talent that exists outside the U.S., and DOE and its laboratories also take careful measures to reduce risk and protect investments in these technologies.

As an entrepreneur, I know firsthand the importance of creating and sustaining an innovation pipeline that starts with funding for fundamental R&D for new discovery, followed by industry-informed R&D to build deployable systems, followed by technology transfer and commercialization for market impact. New science and technology cannot effectively move through the pipeline without deep, mutually beneficial partnerships.

As an example of enabling partnerships in the quantum field, ORNL is performing quantum-based secure communication experiments in collaboration with the Electric Power Board of Chattanooga, the University of Tennessee at Chattanooga, and Qubitekk, Inc., a quantum networking company in California. The goal is to develop resilient quantum network communication in the presence of real-world interference sources such as wind, temperature variations, and vibration. We are leveraging the optical fiber in the EPB commercial quantum network deployed in Chattanooga. DOE's Office of Advanced Scientific Computing Research (ASCR) is investing in R&D for quantum networking at several of its national labs, including Fermi National Accelerator Laboratory, ORNL, and ANL. On the quantum computing front, ORNL is partnering with U.S.-based quantum computing companies through the ASCR-supported Quantum Computing User Program (QCUP). A goal of QCUP is to learn to integrate classical leadership computing systems such as Frontier with commercial quantum computers to enable hybrid classical-quantum computers of the future that can solve complex problems faster and with less energy demand. On a related note, Quantum Brilliance, Inc., just announced a new partnership with ORNL to deploy one of its new quantum computers in our datacenter, enabling additional research for hybrid classical-quantum computing. [https://www.hpcwire.com/off-the-wire/quantum-brilliance-partners-with-ornl-to-integrate-diamond-quantum-computing-into-hpc-systems/] These types of deep partnerships and the ability to deploy large-scale infrastructure to solve challenges are a strength of the national labs. Finally, DOE's five National Quantum Information Science

Research Centers are driving innovations in quantum computing, communication, sensing, and materials, and these centers include partnerships among 115 institutions across North America and Europe. [https://nqisrc.org/]

To maintain U.S. leadership in AI, partnerships among government, national labs, industry, and academia are also critical. DOE labs and industry each have unique and essential ingredients to accelerate AI innovation and transition into practice in a safe, secure, and trustworthy manner. DOE has world-leading facilities for HPC, unique data-generating experimental facilities, deep subject-matter expertise in science and energy, and access to classified national security challenges and associated classified datasets. On the other hand, industry is exponentially investing in rapid, agile, and innovative development of AI hardware and software. Hence, a tight partnership between DOE and industry is important to maintain U.S. leadership in AI for scientific discovery, energy innovation, and national security. Finally, AI workforce development is essential on several fronts, including development of AI researchers who work at the bleeding edge of AI innovation; AI practitioners who leverage and transition new AI tools effectively for their domain of expertise; and AI system engineers who install, maintain, and secure operational AI systems. Our university partners play an essential role in educating the next generation of AI talent and partnering with industry and national labs to provide students with internships and fellowships where they can put their AI education into practice in the laboratory and real-world systems.

An example of a public-private partnership advancing the cybersecurity of OT systems components for the electric grid is the Cyber Testing of Resilient Industrial Control Systems (CyTRICS), funded by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The CyTRICS mission is "protecting the nation's critical energy assets through cybersecurity vulnerability testing, forensic analysis, and subcomponent enumeration." [https://cytrics.inl.gov/] The CyTRICS partnership includes six national labs, led by Idaho National Laboratory (INL), and six industry partners providing OT equipment for the energy industry. CyTRICS is effective at identifying complex cyber vulnerabilities in OT equipment because of this close partnership between labs and industry. Additionally, CESER is supporting regional cybersecurity partnerships such as Auburn University's Southeast Region Cybersecurity Collaboration Center on which ORNL is a key partner. Additional regional partnerships are needed across the U.S. along with corresponding regional electric grid cyber testbeds such as those deployed at INL that enable rigorous R&D and testing of the latest cyber threats to our critical infrastructure. Regional cybersecurity partnerships across the U.S. that coordinate with one another and are also connected via a national cybersecurity coordination network will be a powerful way to mitigate cyberattacks against our electric grid. A current example of a recently launched national cybersecurity coordination network is the Energy Threat Assessment Center (ETAC) in Denver, Colorado, a

CESER-funded government-industry partnership. Tying this cybersecurity theme back to AI and quantum, we need to develop AI-driven, dynamic cyber defenses that can learn and adapt faster than our adversaries can, as well as cyber-impenetrable quantum networks focused on the unique regional needs of the electric grid across the country.

In summary, the cross-disciplinary nature of AI, quantum, and cybersecurity and the associated grand challenges before us motivate partnerships across the government, the DOE national laboratory system, industry, and academia to accelerate the pace of innovation. DOE has demonstrated its commitment to advancing basic and applied research and technology transition across all three of these important technology areas, and DOE can effectively balance the revolutionary opportunities that will come from advancement across these emerging technologies while balancing the associated risks.

Thank you once again for the opportunity to testify, and I welcome any questions you may have on these important topics.