TESTIMONY OF DR. GERALDINE RICHMOND,

PRESIDENTIAL CHAIR IN SCIENCE AND PROFESSOR OF CHEMISTRY

UNIVERSITY OF OREGON

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES

UNITED STATES SENATE

REGARDING

HEARING TO EXAMINE RESEARCH SECURITY RISKS POSED BY FOREIGN NATIONALS FROM COUNTRIES OF RISK WORKING AT THE DEPARTMENT OF ENERGY'S NATIONAL LABORATORIES AND NECESSARY MITIGATION STEPS

FEBRUARY 20, 2025

INTRODUCTION

Chairman Lee, Ranking Member Heinrich, and distinguished Members of the Committee, thank you for this opportunity to testify before the Committee on the important subject of protecting the integrity of the U.S. research enterprise from inappropriate foreign influence. As a lifelong scientist, researcher, and educator, I can attest to the critical importance of this topic for maintaining the nation's competitive edge in science and technology, ensuring that our research efforts remain secure and beneficial to the American public.

I currently serve as Presidential Chair and Professor of Chemistry at the University of Oregon (UO), where I have been a faculty member since 1985. Bridging the fields of chemistry and physics, my research focusses on understanding the molecular characteristics of liquid surfaces, studies that have relevance to issues, such as oil recovery and remediation, atmospheric chemistry, and energy production. Over 200 publications have resulted from the studies conducted in my laboratory with many amazing undergraduate, graduate students and postdoctoral associates. I am also the Founding Director of COACh, a grass-roots organization that has helped over 26,000 scientists and engineers in career advice and advancement in the U.S. and in over two dozen countries around the globe since 1997.

The success of my research and education efforts have led to my election as a member of the U.S. National Academy of Sciences and the American Academy of Arts and Sciences, as well as being honored by many recognitions and awards that began in 1985 with a Presidential Early Career Award from President Reagan, and more recently include the National Medal of Science (2016), the Priestley Medal from the American Chemical Society (2018), the Linus Pauling Medal Award (2018), and Othmer Gold Medal (2023). In addition to serving on many national and international advisory boards, I have

served as elected President of the American Association for the Advancement of Science and Sigma Xi, the Scientific Research Honor Society.

My service to the nation includes appointments to the National Science Board by both President Obama (2012-2018) and President Trump (2018) and the U.S. Science Envoy for the Lower Mekong River Countries (2015-2016) by the Secretary Kerry of the U.S. State Department. Most recently, I served as the Under Secretary for Science and Innovation at the U.S. Department of Energy (DOE) from November 9, 2021-January 20, 2025. In this role, I oversaw the entire portfolio of activities across DOE's Office of Science, the nation's largest federal sponsor of basic research in the physical sciences, DOE's Applied Energy Programs, and 13 DOE National Laboratories. These experiences, both national and international, have provided me with a deep understanding of the scientific and engineering enterprise in this country, but even more, its power to solve our problems and improve our lives. It has also allowed me to observe and experience the changing nature of scientific collaborations and competition with scientists and engineers in other countries over the past four decades.

DEPARTMENT OF ENERGY RESEARCH, TECHNOLOGY, AND ECONOMIC SECURITY INITIATIVES UNDER THE BIDEN ADMINISTRATION

The United States has long been a global leader in scientific discovery and technological innovation. Our research institutions, funded by both public and private investment, have produced countless breakthroughs that drive economic growth, enhance national security, and improve the lives of all Americans. However, as the global competition for knowledge intensifies, so do the threats to our research ecosystem. Hostile foreign governments, malign actors, and cyber threats pose significant risks to U.S. innovation, intellectual property, and the integrity of our research enterprise.

As Under Secretary for Science and Innovation, I led the research security efforts for the Department of Energy during the previous administration. Research security has been a priority for the Department for decades, with policy questions that date back to the Atomic Energy Commission and the secrecy associated with the Manhattan project. The Department has a responsibility to engage in the necessary due diligence and oversight mechanisms to ensure integrity in its programs and to be responsible stewards of the taxpayer dollar. With the enactment of the *Infrastructure Investment and Jobs Act* (also known as the Bipartisan Infrastructure Law, or BIL) and *Inflation Reduction Act* (IRA), which provided more than $62 billion for programs under the purview of the Department of Energy, as well as the *Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act*, it is more important than ever for the Department to have a comprehensive and rigorous approach to research, technology, and economic security (RTES) policy and procedures for its financial assistance awards and loans.

Under the previous administration, DOE developed, and improved upon, a number of RTES measures to mitigate risk that malign foreign governments pose to our scientific and technological development ecosystem, supply chains, and intellectual property. To ensure a robust RTES approach, DOE took three major actions to address the many forms of RTES risks. First, DOE enhanced its existing due diligence processes to ensure that risks of undue foreign influence are considered early in the competitive process and throughout the life of a DOE-supported project or loan. DOE also included strict RTES requirements for its financial assistance and loan programs. For example:

- No person participating in a foreign talent program sponsored by a country of risk may participate in a project.
- Entities applying for funding must be fully transparent regarding foreign connections associated with individuals and entities proposed to participate in the project. Transparency includes sharing sources of intellectual property, foreign collaborations related to the project scope, foreign ownership, and foreign affiliations. Continued transparency is required during the life of a project.

Second, DOE established a department-wide RTES Policy working group to review, develop, and assist in the implementation of RTES policies. Third, the Department established a new RTES Office to implement and continue to evolve DOE's enhanced due diligence process for financial assistance and loan projects, build awareness internally within DOE on RTES issues, engage with external stakeholders, and review DOE national lab agreements involving foreign entities.

RTES Due Diligence Process

For grants and cooperative agreements, the RTES review occurs at three primary phases in the program lifecycle:

- **Phase 1:** A review is conducted on Notice of Funding Opportunity announcements (NOFOs) prior to publication. This ensures that appropriate language is included in the published document, such that potential applicants understand the RTES-related requirements and/or reviews their projects will be subject to.
- **Phase 2:** Prior to selection, a review is conducted of applications that are more likely to be considered for selection.
- **Phase 3:** For funded projects, an RTES review may be triggered in situations where there are changes to the project, personnel, or ownership/control changes that could affect RTES.

A key aspect of the Department's due diligence process is recognizing that addressing RTES risks is the responsibility of the entire Department, not a single office. While the RTES Office serves as a central resource to support the program offices in addressing RTES, part of the RTES Office's mission is also to build awareness internally within DOE. Doing so leverages the resources across DOE to identify potential RTES concerns and does not isolate the responsibility to a single office. It is critical to ensure that each DOE project team of technology managers, project officers, and contracting officers are equipped to understand the RTES concerns, to identify potential concerns as they carry out their merit reviews, review award packages, and monitor ongoing projects. The enhanced due diligence process also relies on the support of the DOE's Office of Intelligence and Counterintelligence, DOE's Committee on Foreign Investment in the United States (CFIUS) Office, and business intelligence tools.

Enhanced Research Security at National Labs

During the previous administration, DOE 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 concerns associated with economic and/or international competitiveness that do 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 the 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. As this Committee 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 activities includes 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.

Risk-based protections must also extend to the intellectual property (IP) developed with federal funding to establish secure and resilient domestic supply chains and maintain U.S. technological competitiveness and leadership. That is why under the previous administration, a comprehensive internal review of the IP licensing practices at DOE National Laboratories was conducted, and policies were developed to apply targeted risk mitigations and monitoring standards, including enhanced DOE oversight, to IP. These changes more effectively ensure that licenses to IP owned by DOE National Laboratory contractors benefit the U.S. economy and protect U.S. economic and national security interests.

The Department of Energy's National Laboratories are the premier engines of scientific discovery and energy innovation, playing a vital role in advancing economic and national security interests. These labs drive cutting-edge research in fields, such as renewable energy, nuclear security, and artificial intelligence, fostering technological breakthroughs that strengthen the nation's economic and defense capabilities. By collaborating with academia, industry, and government agencies, the National Laboratories help maintain U.S. leadership in science and technology while addressing global challenges and ensuring American energy independence.

It is crucial that DOE continually evaluates the effectiveness of research security policies for National Laboratories and improve procedures to maximize security for sensitive laboratory information while minimizing negative impacts to critical collaborative efforts among the global scientific community. Similarly, federal agencies, including DOE, should continue to ensure federal science and technology funding includes strong research security protections to safeguard American innovation, prevent intellectual property theft, and ensure that taxpayer dollars benefit the United States—not foreign competitors.

UNIVERSITY RESPONSE TO RESEARCH SECURITY CONCERNS

Research security concerns have led to the development of policies and procedures at DOE laboratories that have had to evolve with time, even as early as the Manhattan Project. National security is not only the DOE mission; it is also in the culture of practice at the laboratories. For most U.S. research universities this is a newer paradigm as directed by the National Security Presidential Memorandum 33 (NSPM-33) and accompanying guidance, which requires institutions that receive more than $50 million per year in federal science and engineering support to operate a research security program. [4,5]

Universities across the country have adopted effective practices to secure research, protect against intellectual property theft and academic espionage, and prevent undue foreign government influence or infringement on core academic values.[6,7] However, universities cannot do this alone. Federal leadership is crucial in confronting research security concerns and providing the necessary support and guidance to safeguard our nation's academic and research institutions.

At the University of Oregon, we understand these threats fully and are in compliance with NSPM-33. UO's compliance strategy encompasses several key initiatives:

1. **Cybersecurity Program:** UO's Information Security Office offers services such as vulnerability scanning, security consulting, and incident response to safeguard research data. The Export Control Officer and Sponsored Projects Services collaborate to identify projects requiring enhanced cybersecurity controls and communicate these needs to principal investigators.
2. **Foreign Travel Security Training:** UO is developing Foreign Travel Security Training for principal investigators, co-principal investigators, senior/key personnel, program directors, co-program directors, project managers, and any others specified in funding opportunities who will travel internationally for organization business, teaching, conference attendance, or research purposes.
3. **Research Security Training:** Effective May 1, 2025, UO mandates that principal investigators, co-principal investigators, senior/key personnel, program directors, co-program directors, project managers, and others specified in funding opportunities complete annual Research Security Training. The training will ensure researchers understand all federal requirements enforced to protect U.S. research and intellectual property.
4. **Export Control Training:** Effective May 1, 2025, researchers on sponsored awards who perform research and development involving export-controlled technologies must complete Export Control Training. UO offers export control training to ensure compliance with federal regulations governing the transfer of certain items, software, equipment, and information to foreign countries and individuals.

In the wake of NSPM-33, UO's Office of the Vice President for Research and Innovation created a new administrative unit, Research Integrity, led by an Assistant Vice President for Research Integrity and Associate Director of Conflicts of Interest and Export Controls. The individuals in these positions closely track NSPM-33 related guidance and disseminate key updates to campus partners. The work of this team includes a new campuswide Export Control Management Plan and a quarterly convening of campus partners in a National Security in Research Committee. By implementing these measures, the University of Oregon aims to uphold the integrity of its research enterprise while adhering to federal mandates outlined in NSPM-33.

The University of Oregon is not alone in this effort. Other research institutions and universities across the country are also actively addressing the evolving threat of malign influence and working diligently to protect American taxpayer investment in science and technology.

ADDRESSING RESEARCH SECURITY CONCERNS WHILE CONTINUING AMERICA'S COMMITMENT TO OPEN SCIENCE

It is clear that addressing these challenges requires a balanced approach that secures U.S. research while preserving the principles of openness and collaboration that have made our research enterprise successful. Over the past several years, Congress has passed legislation to address research security concerns. During my time as DOE Under Secretary, we worked diligently with the White House, interagency working groups, and Congressional committees of jurisdiction to develop, adjust and upgrade the Department's research security posture in response to Congressional directives, including the *CHIPS and Science Act*, the *SBIR and STTR Extension Act* of 2022, the *National Defense Authorization Acts (NDAAs) for Fiscal Years (FYs) 2020, 2021, and 2025*, as well as Presidential directives such as NSPM-33. For instance, the Department enforced the CHIPS and Science Act's authorization of the S&T Risk Matrix, a crucial risk management tool in the Department's research security toolkit. In addition to the RTES Office, the cross-cutting RTES Policy Working Group will steward and shape the Department's research security policy approach to ensure compliance with Congressional requirements.

At my time of departure, the Department was engaging with the National Science and Technology Council (NSTC) Research Security Subcommittee on common disclosure forms for senior/key researchers, pursuant to section 223 of the FY 2021 NDAA and NSPM-33, to ensure consistency with legal requirements and agency authorities. DOE was also preparing to enforce language banning foreign nationals from China, Russia, North Korea, and Iran from accessing the National Laboratories operated by the National Nuclear Security Administration (NNSA) without Secretarial waivers, pursuant to Section 3112 of the FY 2025 NDAA. This provision will take effect on April 15, 2025. Moreover, the FY 2025 NDAA requires quarterly reporting to Congress on the number of covered foreign nationals seeking access to all 17 DOE laboratories. This is set to begin 90 days after the bill's enactment. While I cannot speak to the status of these activities in my current capacity, I can reassure the Committee that, regardless of the administration, the Department takes its responsibility to protect the scientific integrity of our nation's assets seriously.

As this Committee is evaluating research security measures of U.S. science and technology research enterprise, I offer the following recommendations:

1. **Enhanced Security Coordination:** Congress should take steps to encourage coordination between the research security practices and policies of our National Laboratories and universities while recognizing their distinct missions. Research at National Laboratories focuses on applied, mission-driven projects related to national security, defense, and emerging technologies, often involving high-security concerns. In contrast, universities prioritize fundamental research across a wide range of disciplines, typically involving lower-security risks. Not all scientific research areas pose the same level of security concern as many of our emerging technology fields. Tailored safeguards should be implemented to protect critical research without unnecessarily hindering scientific collaboration and innovation.

2. **Incorporating Research Security Measures into Emerging Fields:** To safeguard U.S. technological leadership and national security, Congress should prioritize the early integration of research security measures in emerging fields, such as AI, quantum computing, and fusion energy. DOE's National Labs are crucial in advancing these fields, driving groundbreaking innovations that shape the future of energy, defense, and advanced computing. To protect these critical technologies, support for the National Labs should include dedicated funding for research security initiatives, strengthening safeguards against intellectual property theft and foreign influence, and bolstering supply chain protections.

3. **Investing in a Robust STEM Workforce:** Foreign-born professionals make up a substantial portion of the STEM workforce. They contribute to groundbreaking advancements across various sectors, particularly in high-tech fields and academia. Given the national security and economic advantages of U.S. leadership in science and engineering, U.S. policies must ensure that America remains an attractive destination for foreign STEM talent and that non-citizen foreign-born science and engineering professionals can remain in the U.S. after graduation. Additionally, Congress should focus on expanding opportunities to develop domestic STEM talent across the entire educational and career pipeline, starting from K-12, to strengthen U.S. leadership in science, innovation, and national security.

CONCLUSION

Chairman Lee, Ranking Member Heinrich, and Members of the Committee, thank you again for the opportunity to testify before you today. I look forward to answering your questions.