TESTIMONY OF MR. JEREMY ISON

CHIEF OF STAFF, OFFICE OF THE UNDER SECRETARY FOR SCIENCE

UNITED STATES DEPARTMENT OF ENERGY

HOUSE SELECT COMMITTEE ON THE STRATEGIC COMPETITION BETWEEN

THE UNITED STATES AND THE CHINESE COMMUNIST PARTY

UNITED STATES HOUSE OF REPRESENTATIVES

ON

PROTECTING AMERICAN INNOVATION: THE FEDERAL

RESEARCH SECURITY ENTERPRISE

WEDNESDAY, JULY 15, 2026

Introduction

Chairman Moolenaar, Ranking Member Khanna, and distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss the Department of Energy's (DOE) commitment to research security. At DOE, we view research security concerns with the utmost gravity, recognizing the tangible threat posed by adversaries targeting our research and development ecosystem. This threat specifically targets our National Laboratories as well as our academic and private-sector grant recipients and directly undermines our national security and competitive advantages. We are also actively working to address foreign talent and supply chain dependencies from countries of risk such as the People's Republic of China (PRC). We are doing so through risk-informed mitigation protocols and a

deliberate strategy to expand American Science, Technology, Engineering, and Mathematics (STEM) talent and secure domestic supply chains to meet our research and development needs. We deeply appreciate the partnership of this committee in helping safeguard American innovation.

The United States (U.S.) has long maintained its global leadership in science and technology (S&T) through the unique strengths of its collaborative scientific enterprise. The Department is working to mitigate the inherent risks of international collaboration while simultaneously extending America's competitive S&T edge. Our approach is characterized by a deliberate and risk-informed balance: mitigating risks in an evolving threat landscape while fostering the research environment essential for continued innovation. This balance is crucial, as the DOE National Laboratories serve as engines of innovation contributing significantly to the nation's S&T capability and capacity. This testimony will outline the Department's framework for achieving this balance.

Background and Historical Context

For decades, the U.S. government's approach to fundamental research rested on a clear premise: when national security controls were required, they would be applied through classification or other formal control mechanisms, while the conduct and reporting of fundamental research would remain unrestricted. That model helped the United States build the world's leading research enterprise, but it does not fully account for today's reality: unclassified does not always mean low risk, especially when the work involves technology areas that strategic competitors have identified as national priorities. The PRC has sought to exploit that gap – and this Committee has documented cases where it has done so – through state-directed efforts to acquire foreign science and technology. That exploitation continues through malign talent recruitment programs, defense-linked research institutions, opaque foreign obligations and ownership structures, and ostensible academic collaborations designed to serve PRC priorities.

DOE recognized these risks before the current government-wide research security framework was fully in place, building on a Departmental security infrastructure that long included counterintelligence and foreign national access controls. As early as 2004, DOE first issued Order 142.3, establishing requirements for foreign national visits and assignments through the Foreign National Access Program, and in January 2017, issued Policy 485.1 to require review

of specific foreign engagements with the National Laboratories. In 2019, DOE developed and began implementing the Science and Technology Risk Matrix (STRM) to help identify and categorize risks in critical and emerging technology areas and also issued and later updated Order 486.1 to prohibit talent recruitment program participation and restrict participation in foreign government sponsored or affiliated activities. These actions provided the foundation for DOE's early implementation of National Security Presidential Memorandum 33 (NSPM-33), the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, and DOE's Research, Technology, and Economic Security (RTES) framework across its broader financial assistance portfolio.

Mitigating Risk in the Evolving Threat Landscape: DOE's Current Research Security Framework

Despite these early steps, the threat landscape facing U.S. research and development has continued to evolve. The Department has strengthened its approach accordingly, moving from discrete controls toward a layered, risk-based system that identifies concerns early and applies safeguards where they are needed. That system relies on technical and security expertise, clear review processes, analytic tools, and secure research environments to protect taxpayer-funded research while preserving the strengths of the U.S. research enterprise.

Safeguarding the DOE National Laboratories

A cornerstone of DOE's research security approach is the safeguarding of its National Laboratories, which form the backbone of America's scientific leadership and national security, groundbreaking discoveries, and the development of critical technologies. They operate with a deeply embedded culture of maintaining national security, utilizing a deliberate Managed Research Environment (MRE) structured by Departmental Directives. By integrating specialized security personnel, standardized operational procedures, physical and digital protective tools, and collocated counterintelligence infrastructure, our MREs provide risk-informed physical and electronic security that protects sensitive and classified work while maintaining the collaborative environment required for scientific research.

One essential component of this overarching risk management framework is determining who gains access to our laboratories. Foreign nationals requesting access to a National

Laboratory, whether visitors or employees, undergo indices checks and some additional counterintelligence vetting for those from sensitive countries. Through the counterintelligence program, the Department has successfully piloted and moved to implementation of a new Risk Management Framework (RMF) for vetting foreign nationals. The RMF is a method to assess the threats that foreign visitors may pose to DOE facilities, including National Laboratories. The RMF applies threat assessment standards established by law and DOE procedure to enable the Department to balance the conduct of science with the protection of sensitive information and technologies. To ensure the rigor of these processes, DOE recently updated its directive governing unclassified foreign national access to the National Laboratories through DOE Order 142.3C. This update implements Section 3112 of the Fiscal Year 2025 National Defense Authorization Act (NDAA) and institutes a new Supplemental Questionnaire to enforce more rigorous vetting for unclassified visits across the broader laboratory system, amongst other changes.

Personnel access controls at the National Laboratories provide an important layer of protection by limiting foreign national access to sensitive information, facilities, systems, and technologies based on risk, affiliation, and mission need. Beyond personnel access controls, our facilities leverage physical and digital tools to protect sensitive research from foreign acquisition. This includes leveraging closed work environments to physically and electronically isolate sensitive, classified research, supplemented by export controls to prevent the unauthorized transfer of critical technology. An additional integral tool in this effort is the STRM, which was developed by DOE and the National Laboratories in 2019 and was updated this year. The STRM identifies and categorizes risks in unclassified critical and emerging technology areas such as Artificial Intelligence (AI) and Quantum Information Science (QIS), guiding the appropriate controls applied to foreign engagements.

Providing analytical support for these tools and procedures is DOE's dedicated Counterintelligence (CI) program within the Office of Intelligence and Counterintelligence (IN). Collocated directly at field offices across the National Laboratories, CI personnel provide essential, embedded risk assessment and mitigation capabilities. The CI program supports laboratory leadership in making informed decisions about foreign engagements, conducts defensive briefings, and investigates potential foreign threats to DOE equities, playing a critical role in safeguarding sensitive information.

DOE's swift implementation of Section 3112 of the Fiscal Year 2025 NDAA demonstrates how this integrated framework responds to immediate national security mandates. This statutory provision restricts access to non-public areas of certain covered facilities, including National Nuclear Security Administration (NNSA) laboratories and other sites associated with nuclear weapons production and nuclear propulsion, by citizens of the People's Republic of China, Russian Federation, Democratic People's Republic of Korea, and Islamic Republic of Iran. Upon passage of the Act, NNSA used its review processes to evaluate covered foreign nationals who were employed or sought access to covered NNSA facilities. This comprehensive review resulted in covered individuals at the three NNSA laboratories having their access revoked except for three individuals who were granted waivers consistent with the requirements of Section 3112. This demonstrates DOE's commitment to Congressional directives focused on safeguarding the most sensitive areas of our national security enterprise, particularly within the distinct risk environment of NNSA.

In summary, these mitigations allow us to benefit from global scientific talent while ensuring that sensitive capabilities are protected from unauthorized disclosure or diversion.

Protecting Taxpayer Investments in DOE-Supported Projects

Our commitment to protecting taxpayer investments extends to DOE's strategic funding of external projects, funded through grants, cooperative agreements, loans, prizes, and similar funding mechanisms to universities and other institutions. To achieve affordable, reliable and secure energy, we must take critical actions to support innovation. Unfortunately, foreign adversaries seek to exploit U.S. science and technology investments to advance their own military, economic, or technological capabilities. To protect against these risks, the (RTES Office conducts due diligence reviews of these funds to identify potential risks of interference by malign foreign actors, intellectual property loss, supply chain dependencies, and risks to national security and economic competitiveness. The risk-based due diligence process is closely coordinated between the RTES Office and the IN. The process also relies on the science and technology expertise of the program offices. Based on its findings, the RTES Office provides a recommendation to the program office and where appropriate, develops mitigations to address potential risks.

Our core goals are straightforward: to make risk-based decisions that minimize potential intellectual property loss, protect our supply chains, and guard against threats to our national and economic security, thereby ensuring taxpayer dollars strengthen America and not our adversaries. Simultaneously, we demand full transparency from our researcher community. Individuals and entities applying for DOE support must be fully forthcoming regarding foreign connections, particularly regarding connections involving foreign countries of concern. Full disclosure allows us to identify and address potential risks upfront, effectively protecting public funds and preventing the diversion of research.

Our RTES due diligence review process for these decisions unfolds in a series of consecutive evaluations throughout the funding cycle from initial solicitation through project completion.

This review process begins in Phase 1 with upfront assessments of Notices of Funding Opportunity and other solicitations prior to publication. This ensures that solicitations contain clear security language and that potential applicants understand all compliance requirements. DOE is unique among federal agencies in its broad portfolio, ranging from fundamental research to large-scale energy projects that impact critical U.S. infrastructure. We apply "right-sized" security requirements, meaning controls are appropriate and effective for the specific level of risk, whether it involves early-stage academic research or large-scale energy deployment.

Following solicitation, Phase 2 involves systematic due diligence reviews of applications. This process includes evaluating technical proposals, biographical data, current and pending support disclosures, and transparency of foreign connections disclosures. Our assessments examine risk factors related to individuals' and entities' foreign affiliations, prior activities, and the sensitivity of the technology involved. We specifically scrutinize any affiliations that could facilitate unauthorized transfer of intellectual property or expertise. As part of the assessment for *individuals*, DOE considers ties to malign foreign talent recruitment programs, foreign funding sources (both monetary and in-kind), concerning behaviors associated with patenting (e.g., transferring to foreign entities after filing), and ties to foreign entities or foreign collaborators on U.S. restricted party lists, with military connections, or with specified characteristics. For *entities*, DOE considers foreign ownership or control, relationships with

foreign countries of concern (e.g., joint ventures, licensing, supplier relationships, etc.), patent history, military connections, and other ties to entities on U.S. restricted party lists.

Once an award is made, Phase 3 involves monitoring throughout the life of the project. Because changes in personnel, project scope, an entity's ownership and new foreign connections can alter a project's risk profile, recipients must notify the Department of these updates. The RTES Office conducts ongoing due diligence to verify this information, taking a risk-based approach to monitoring and ensuring the long-term integrity of the funded research.

Throughout this process, our concern is protecting against the actions of certain countries, including the PRC. To demonstrate the Trump administration's commitment to research security, DOE has taken substantive steps since January 2025 to improve our risk-based approach to research, technology and economic security. Many of these steps align with this committee's recommendations. As part of the due diligence review process, DOE is now implementing additional monitoring protocols during the project period. DOE strengthened the Transparency of Foreign Connections disclosures for entities seeking to participate in a DOE-supported project and the disclosures for individual researchers. For example, in higher risk technology areas, DOE implemented a disclosure form that requires up to a 10-year look-back from researchers. DOE also strengthened security-related award terms, expanded the Entity of Concern prohibition, and incorporated the Uyghur Forced Labor Prevention Act Entity List in our due diligence processes. DOE was also the first Department to require the research security training mandated in the CHIPS and Science Act. As new statutory requirements are enacted, DOE is committed to expeditiously implementing those statutory requirements.

Maintaining America's Competitive S&T Edge

America's S&T leadership depends not only on protecting the capabilities we possess today, but on pioneering what comes next. Rapid advances in fields such as AI, QIS, and biotechnology require a research environment that is both secure and innovative.

The DOE National Laboratories remain at the forefront of research in these strategic and emerging technologies. Our National Laboratories—spanning both the NNSA, the applied programs and the Office of Science—collectively advance our national security and fundamental scientific research missions. Success in these endeavors depends upon our ability to cultivate and attract exceptional scientific talent while distinguishing between unacceptable risk and

legitimate, mission-aligned collaboration. It is through a risk-informed approach that the Department maintains this balance.

Recognized Challenges and Areas for Improvement

Despite the Department's ongoing security enhancements, certain challenges persist within the broader research and development landscape, presenting opportunities for further strengthening our collective security posture.

One challenge lies in the variance of research security awareness and training across the U.S. research ecosystem. In particular, academic institutions do not always possess a consistent and granular understanding of foreign exploitation tactics. This disparity can create vulnerabilities that foreign adversaries actively seek to exploit. While there is always more to do, DOE has co-funded the U.S. government's research security training modules that were developed in response to NSPM-33. These cooperative initiatives are vital for enhancing awareness and preparedness across the entire federal research enterprise.

The Department of Energy is steadfast in its commitment to continuously strengthening our research security posture as we adapt to evolving challenges and identify areas for enhancement. We acknowledge the findings within the House Select Committee on the CCP's "Containment Breach" report and are undertaking a comprehensive review of the Department's approach to research security. This review examines our organizational structure, roles, responsibilities, and processes to ensure we are developing the most effective and efficient approaches to vetting and due diligence. We intend to build upon our recent successes in strengthening the vetting processes for foreign nationals, applying those lessons to fortify other areas, such as financial due diligence reviews.

The Path Forward

To effectively address these challenges and navigate the evolving landscape of research security, the Department has aligned with the Committee's expressed priorities and focuses on three strategic pillars.

First, DOE is prioritizing the continued development and implementation of tailored and risk-based strategies for foreign national access and collaboration. Such an approach, by concentrating enhanced controls where the risk is demonstrably highest, prevents

undifferentiated, blanket prohibitions that could harm America's scientific enterprise and its leadership position. Concurrently, we must work continuously to provide clear, uniform, and actionable guidance for all DOE research funding recipients.

Second, DOE will work to enhance federal capabilities for conducting advanced analytical vetting and monitoring research security risks. These tools are increasingly vital to efficiently process complex disclosure information, identify anomalies, and proactively detect evolving foreign exploitation patterns. At the same time, the Department cannot achieve this security posture in isolation; we must share these due diligence findings and risk assessments across the federal government, ensuring that adversarial actors cannot exploit communication gaps between funding agencies.

Finally, we assert that the most effective long-term strategy is to out-innovate and out-educate our adversaries by systematically building our domestic talent. To ensure America's research enterprise is powered, first and foremost, by American talent, we must treat the cultivation of domestic STEM talent as a national security priority. By aggressively developing our own American human capital, we secure our scientific pipeline and ensure that America's most sensitive, pioneering research is led by a workforce fully aligned with our national interests.

Conclusion

In closing, the Department of Energy views research security as among its highest priorities. We are committed to a balanced, proactive, and continuously improving approach to protect our nation's scientific enterprise. Central to the effort is our long-term commitment to aggressively promoting and recruiting domestic STEM workforce. We are confident in our research security frameworks, our transitioning workforce pipelines, and the deep expertise within our university grant programs and National Laboratories, and we remain dedicated to working closely with Congress to ensure that America not only maintains, but further strengthens, its leadership in science and technology.

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