TESTIMONY OF JAY TILDEN,
DIRECTOR
OFFICE OF INTELLIGENCE AND COUNTERINTELLIGENCE
U.S. DEPARTMENT OF ENERGY

BEFORE THE
OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES
ON
RESEARCH SECURITY: EXAMINING THE IMPLEMENTATION OF THE CHIPS AND SCIENCE ACT AND NSPM-33

THURSDAY, DECEMBER 18, 2025

Introduction

Chairman McCormick, Ranking Member Sykes, and distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss the Department of Energy's (DOE) unwavering commitment to research security. At DOE, we view research security concerns with the utmost gravity, recognizing the tangible threat posed by the diversion of legitimate, taxpayer-funded research for malign purposes. This threat encompasses not only economic loss and the erosion of our nation's competitive advantage but also, critically, the possible compromise of national security interests.

The United States has long maintained its global leadership in science and technology (S&T) through the unique strengths of its collaborative scientific enterprise. DOE is working to manage the inherent risks of international collaboration while simultaneously maintaining America's competitive S&T edge. Our approach is characterized by a deliberate 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 in particular serve as unparalleled engines of innovation contributing significantly to the nation's S&T prowess. This testimony will outline DOE's framework for achieving this delicate balance.

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

The threat landscape facing U.S. research and development is dynamic. Certain foreign governments, notably the People's Republic of China, actively exploit our scientific ecosystem. DOE has continuously strengthened its research security approach in response. Our

comprehensive, multi-layered approach integrates expert personnel, robust procedures, advanced tools, and critical infrastructure to safeguard taxpayer-funded research.

Safeguarding the DOE National Laboratories

A cornerstone of DOE's research security framework is the rigorous safeguarding of DOE's National Laboratories, which are a key component of America's scientific leadership and national security. They are the sites of groundbreaking discoveries and the development of critical technologies. They operate with an inherent, deeply embedded culture of maintaining national security, functioning as a robust managed research environment. This environment meticulously balances risk with benefit, continuously evolving with changing threats, and enables both classified and unclassified research, even on sensitive technologies, to occur alongside fundamental research where international engagement is often essential.

It is important to note that there are distinct missions and corresponding risk profiles across the 17 DOE National Laboratories. The 3 National Nuclear Security Administration (NNSA) Laboratories have primary missions focused on nuclear weapons stewardship and national security, often involving classified work and a distinct risk posture that mandates the highest levels of security. In contrast, the Office of Science (SC) laboratories are leaders in fundamental scientific research, spanning fields from high-energy physics to high-performance computing, and host thousands of researchers from around the world at their scientific user facilities. While their primary missions and risk profiles differ, all 17 DOE National Laboratories adhere to a rigorous, integrated security framework, consistent with National Security Presidential Memorandum (NSPM)-33 implementation and thereby serve as a comprehensive model for managing diverse risk profiles in critical research environments. Indeed, DOE is working aggressively to issue a comprehensive directive to the laboratories that leverages their existing risk management posture to meet NSPM-33's research security program requirements. To do so, our managed research environment relies on world-class security and technical leadership, clear and risk-informed policies, and robust controls and procedures.

We maintain strict controls over access. All foreign nationals are vetted with indices checks, and those from sensitive countries may undergo additional counterintelligence scrutiny. Access is also revocable if the risk-benefit ratio changes. The Department of Energy vigorously pursues the evaluation and enhancement of policies designed to counter risks posed by foreign national access.

Our facilities utilize advanced tools, including closed work environments and export controls to protect technologies from theft. The Science and Technology Risk Matrix (STRM), developed in 2018, identifies and categorizes risks in emerging areas such as Artificial Intelligence (AI) and Quantum Information Science (QIS), guiding foreign engagement controls.

DOE's dedicated Counterintelligence (CI) program provides essential risk assessment and mitigation within the labs, informing leadership decisions and investigating foreign threats to the Department.

Further, DOE swiftly implemented Section 3112 of the National Defense Authorization Act for Fiscal Year 2025. This restricted access for citizens of the People's Republic of China, Russian Federation, Democratic People's Republic of Korea, and Islamic Republic of Iran to non-public areas of NNSA facilities. This demonstrated DOE's commitment to Congressional directives, with waivers granted only consistent with Section 3112 requirements.

Protecting Taxpayer Investments in DOE Grants

Our commitment to safeguarding research extends to grants, cooperative agreements, loans, prizes, and similar funding mechanisms where DOE invests in external projects. DOE's Research, Technology, and Economic Security (RTES) framework continually minimizes, mitigates, and manages risks. Our core goals are to minimize intellectual property loss, protect supply chains, and guard national and economic security, ensuring taxpayer dollars benefit America. We require full transparency from researchers and entities regarding their collaborations with foreign research personnel and entities, particularly with countries of concern or foreign talent programs.

DOE applies "right-sized" security requirements, appropriate for the specific level of risk from early-stage academic research to large-scale energy projects.

Our rigorous RTES due diligence review unfolds in three phases, coordinated by DOE's specialized RTES Office with support of subject matter experts from Intelligence and Counterintelligence. This team actively collaborates with subject matter experts from DOE and NNSA Program Offices to lend their expert insight into the risks and implications of specific science and technology areas across three phases during the lifetime of a grant.

- **Phase 1:** Upfront assessments of funding solicitations ensure appropriate language and applicant understanding of RTES requirements.
- **Phase 2:** Thorough due diligence review of applications before selection, including technical proposals, biographical data, current and pending support disclosures, and transparency of foreign connections disclosures with scrutiny on foreign connections and potential conflicts of interest.
- **Phase 3:** The risk profile can change after a project is selected for funding, so DOE includes two types of reviews during the life of the project, which ensures the continued integrity of the research. First, an RTES review triggered by certain changes such as personnel or ownership. Second, DOE also includes continuous RTES monitoring.

DOE ensures RTES reviews focus on individual behaviors and do not discriminate based on race, color, or national origin, consistent with Title VI of the Civil Rights Act of 1964. When risks are identified, mitigation is prioritized. If not possible, decisive action is taken with due process. The decisive action may include removal of organizations or key personnel and other individual project participants from DOE-sponsored projects where the risks of malign foreign influence cannot be sufficiently mitigated

The Department of Energy has comprehensively implemented all research security requirements mandated by the CHIPS Act. Our commitment to this predates the Act in several areas; for instance, the prohibition on malign foreign talent recruitment programs for DOE employees and national laboratory contractors has been enforced since 2019. For financial assistance mechanisms, DOE's standard award terms and conditions now fully integrate key CHIPS requirements, including the prohibition on malign foreign talent recruitment programs with annual certifications for covered individuals, recipients, and subrecipients, along with a mandate for prompt notification of any suspected participation. Furthermore, DOE was the first agency to implement the requirement for research security training, necessitating completion by covered individuals within one year prior to application, or within thirty days of joining an ongoing project. We also prohibit Entities of Concern and associated research personnel from receiving DOE funding. To manage these complex issues, the RTES Office has been designated to track and notify recipients of unmanageable threats to U.S. national security or intellectual property loss posed by Entities of Concern, while also facilitating information sharing with other federal agencies and developing consistent identification approaches. Consistent with our RTES Framework memorandum, we deploy risk-based strategies for evaluating, assessing, mitigating, and reporting these risks, all while upholding a strict commitment to non-discrimination, ensuring these policies do not target, stigmatize, or discriminate based on any protected characteristic.

Maintaining America's Competitive S&T Edge

S&T leadership requires both protection and pioneering. The DOE National Laboratories are at the forefront of critical emerging technologies like Artificial Intelligence and Quantum Information Science. Both NNSA and Office of Science labs rely on a global pool of talent.

A portion of U.S. STEM graduate students and postdoctoral researchers are foreign-born and contribute significantly to the American research enterprise. Our policies must ensure the U.S. remains an attractive destination for top STEM talent. While we prioritize domestic talent, attracting the world's most skilled scientists in our labs is crucial to win the race on AI and emerging technologies.

Recognized Challenges and Areas for Improvement

Despite DOE's efforts, challenges persist. A significant one is the variance in research security awareness across the broader federally funded research ecosystem, particularly in academia. This creates vulnerabilities. DOE co-funded research security training modules and strongly supports the National Science Foundation SECURE Center to enhance awareness.

- Furthermore, comprehensive vetting and continuous monitoring require significantly enhanced programmatic oversight and coordination, especially for counterintelligence programs, RTES unclassified due diligence programs, and partner federal research agencies.

The Path Forward

To address these challenges, we offer key considerations for collective attention:

- **Tailored and Risk-Based Strategies:** Continue developing prudent strategies for foreign national access that mitigate risks and enable collaboration for a world leading S&T research ecosystem. This prevents blanket prohibitions and requires clear, uniform guidance for academic institutions, particularly for joint institutes and academic exchanges in dual-use fields. A comprehensive, interagency approach is vital to prevent sensitive knowledge transfer and ease administrative burdens.
- **Enhanced Federal Capabilities:** Strengthen federal capabilities for advanced analytical vetting and continuous monitoring. This requires dedicated counterintelligence and unclassified due diligence programs; state-of-the-art tools like AI and data analytics to process complex disclosures, identify anomalies, and detect foreign exploitation patterns efficiently; and IT systems that can easily connect to each other.
- **Out-Educate and Out-Innovate:** The most effective long-term strategy is to support a robust American-born STEM talent pipeline from K-12 through post-graduate levels, while also leveraging the capabilities of our National Laboratories. This ensures America maintains its competitive edge free from foreign dependency, especially in sectors critical to national security.

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. We are confident in our robust frameworks 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 McCormick, Ranking Member Sykes, and Members of the Committee, thank you again for the opportunity to testify before you today. I look forward to answering your questions.