S. HRG. 119–45

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

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

FEBRUARY 20, 2025

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

60–021 WASHINGTON : 2025

COMMITTEE ON ENERGY AND NATURAL RESOURCES

MIKE LEE, Utah, *Chairman*

JOHN BARRASSO, Wyoming
JAMES E. RISCH, Idaho
STEVE DAINES, Montana
TOM COTTON, Arkansas
DAVID MCCORMICK, Pennsylvania
JAMES C. JUSTICE, West Virginia
BILL CASSIDY, Louisiana
CINDY HYDE-SMITH, Mississippi
LISA MURKOWSKI, Alaska
JOHN HOEVEN, North Dakota

MARTIN HEINRICH, New Mexico
RON WYDEN, Oregon
MARIA CANTWELL, Washington
MAZIE K. HIRONO, Hawaii
ANGUS S. KING, JR., Maine
CATHERINE CORTEZ MASTO, Nevada
JOHN W. HICKENLOOPER, Colorado
ALEX PADILLA, California
RUBEN GALLEGO, Arizona

WENDY BAIG, *Majority Staff Director*
PATRICK J. MCCORMICK III, *Majority Chief Counsel*
JASMINE HUNT, *Minority Staff Director*
SAM E. FOWLER, *Minority Chief Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

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

THURSDAY, FEBRUARY 20, 2025

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

The Committee met, pursuant to notice, at 10:00 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Mike Lee, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. MIKE LEE, U.S. SENATOR FROM UTAH

The CHAIRMAN. The Committee will come to order. The Senate Energy and Natural Resources Committee's hearing on research security risks posed by foreign nationals from countries of risk working at the Department of Energy's national laboratories and necessary mitigation steps. I will give my five-minute opening statement here in a moment. Then, I will turn to Ranking Member Heinrich for his opening statement. Then, I will introduce witnesses and give them an opportunity to give their five-minute opening statements.

The U.S. Department of Energy oversees 17 national labs. These labs have been instrumental in shaping America's technological and military competitive edge. From the Manhattan Project to cutting edge AI research, DOE's national labs have pushed the boundaries of innovation and strengthened our national security. But for those very same reasons, they have also become a prime target for espionage. Secretary Chris Wright, at his confirmation hearing just a few weeks ago, said, "We must protect and accelerate the work of the DOE labs to secure America's competitive advantage and security." I could not agree more. And that is precisely why we are here today at this hearing to explore ways that we can secure American technology for the benefit of our economic and national security.

For years, the Chinese Communist Party has worked to infiltrate our national labs, targeting top scientists and siphoning off American research to fuel China's military ambitions through programs like the Thousand Talents Program. The CCP systematically recruited elite scientists, nationals of the People's Republic of China, who were trained in the West, built their careers in American labs,

and worked with American funding to develop American technology. And then, the CCP lured them back to China. It is a deliberate strategy to leverage U.S. taxpayer-funded expertise for the benefit of the Chinese military, and tragically, we are starting to see the consequences. Former DOE researchers are helping China develop hypersonic missiles, deep earth penetrating warheads, and advanced submarines. These are weapons designed to outmatch and deter the United States. Make no mistake, Beijing is actively exploiting weak security protocols, academic collaboration loopholes, and U.S. grant programs to advance its military capabilities, all on American taxpayers' dime.

During his first term, President Trump tightened DOE's security protocols at the labs. He cracked down on CCP recruitment programs and ensured accountability at the DOE for those who approved a researcher from a country of risk working on DOE projects, making it clear that our national labs wouldn't be used to strengthen the Chinese military. But President Biden loosened those restrictions, and the door is once again open to the CCP, which compels its citizens, by law, to disclose information that they might have that can benefit China's strategic goals. That is unacceptable to the United States. Congress and this Administration must act immediately to close the gaps, tighten security, and ensure that American research stays in American hands.

I am looking forward to understanding how the Department of Energy, under the Biden Administration, allowed foreign adversaries to infiltrate our most sensitive research institutions and exploring ways to ensure this never happens again. If we fail to protect our scientific leadership, our intellectual property, and our national secrets, we don't just lose our competitive advantage, we hand it directly to our greatest geopolitical rival. So I look forward, needless to say, to hearing from our witnesses today and learning more about this emerging problem.

Now we will turn to Senator Heinrich for his opening statement.

OPENING STATEMENT OF HON. MARTIN HEINRICH, U.S. SENATOR FROM NEW MEXICO

Senator HEINRICH. Thank you, Chairman Lee, and thank you to our expert panel of witnesses for coming to speak with us today.

As Ranking Member of the Senate Energy and Natural Resources Committee, and also a member of the Senate Select Committee on Intelligence, counterintelligence at our national labs is a matter that I believe we should all take very seriously. But first, I want to discuss another counterintelligence risk. Last week, the Trump Administration laid off 1,800 DOE employees. Many of our nation's top experts in fields essential to our economic and national security, such as critical and emerging technologies and nuclear safety, were let go. These employees had top security clearances and were dismissed without following legal protocol to end those clearances. And the Trump Administration is now trying to reverse course and reinstate some of these employees. But you have to ask, why would they want to go back after being treated this way? Our best experts have lost trust in the U.S. Government. President Trump is doing exactly what our adversaries want. They aren't losing their best experts, we are. This is a national security threat

that will have lasting impacts on our country for decades to come. I sent a letter to the President urging the Administration to halt these mass firings, and I would encourage my colleagues to do the same.

Turning back to the research security at our DOE national labs, this is a sensitive issue. We want to avoid telegraphing to our adversaries details on the research our labs are doing and what security protocols our national labs take to protect it. We don't want to give our adversaries a blueprint of any vulnerabilities. This is why we have always discussed this issue in a classified setting. And quite frankly, I am disappointed to read some of the witness testimony to which we cannot appropriately respond in this open venue. But we are here today, so let's do our best to take care with how we have this discussion in a public setting.

Additionally, as no one on this panel is currently at DOE or any of the national labs, I think it's important that we be briefed by DOE and its Office of Intelligence and Counterintelligence about how it is implementing recently passed legislation before using this hearing or any hearing as an impetus for future legislation.

Most people think about the Department of Energy for its Manhattan Project beginnings or work advancing energy technologies. But DOE does much more than just nuclear weapons and energy. The Department is also the largest supporter of physical science scientific research in the Federal Government, conducting research and developing technologies across a range of fields, from artificial intelligence, to vaccine development, to astrophysics. The United States has been able to accomplish breakthroughs in space exploration, supercomputing, and the human genome project because of the work at the national laboratories. We have been able to accomplish so much and be the first to do it, in part because of the counterintelligence capabilities we possess that have kept our research safe and secure. The fact that DOE's Counterintelligence Office is under the umbrella of the intelligence community is a critical asset that we must leverage and strengthen.

The threat of foreign espionage is becoming increasingly more complex and dangerous. We need to adapt. When scientists or students from other countries want to come and partake in our world-class research, we must take a serious look at the security risks involved, especially individuals from countries we have deemed a national security concern. On the one hand, we must recognize and embrace that much of America's science and technology 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 computer science doctorates. Between 1901 and 2023, immigrants have been awarded 36 percent of the Nobel prizes won by Americans in chemistry, medicine, and physics. The Department of Energy would not exist without the contributions of Enrico Fermi and Hans Bethe—two immigrants from World War II adversarial nations—to the Manhattan Project.

So we must be sure that we have strong research security safeguards in place while ensuring we can be a home to the best and brightest from around the world. Striking this balance between international cooperation in science and technology and our national security is not easy. In the CHIPS and Science Act, and

more recently in the Fiscal Year 2025 Intelligence Authorization Act, we authorized bipartisan and balanced research security improvements for the DOE that strengthen their capabilities in this space.

So I look forward to hearing about how Congress can best support DOE's efforts in safeguarding our research for the sake of our country's national security. However, as we all know, not all threats come from foreign entities. Thorough background checks are required before any individual has access to sensitive information. In the past few weeks, we have seen multiple instances of staffers from the Department of Government Efficiency—which is not a department—or DOGE, gain access to information systems throughout the Federal Government. We have seen instances of staff being able to access federal payment systems at the Treasury Department, as well as trying to access personal details of Americans at the Social Security Administration. Jay Tilden, the Head of DOE's Office of Intelligence, even had to remind staff that DOGE employees could not have access to SCIFs without a clearance. All of this is concerning. Along with my colleagues on the Senate Select Committee on Intelligence, I sent a letter to the White House demanding answers regarding DOGE operations and their seemingly unfettered access to sensitive information. These are unprecedented risks to our national security, and it is paramount that we address them immediately.

With that, Chairman, I yield back.

The CHAIRMAN. Thank you, Senator Heinrich.

It is, of course, important to remember that the President, under Article II, is vested with the "executive Power," and the President has the authority, constitutionally and statutorily, to decide who can see what within his Administration, and when he designates someone as having access to it, they do have access to that.

I want to thank our witnesses here today. Let me introduce each of them quickly, and then we will turn to each of you for your opening statements.

First, we have Mr. Paul Dabbar. Mr. Dabbar is the co-founder of Bohr Quantum Technology and former Under Secretary of Science at the Department of Energy under the Trump Administration. As Under Secretary of Science, Mr. Dabbar managed the national laboratory complex at the Department of Energy.

Next, we have Ms. Anna Puglisi. Ms. Puglisi is a Fellow at the Hoover Institute, a public policy think tank housed at Stanford University. Ms. Puglisi has testified extensively on this topic we are discussing today. So we will look forward to hearing your thoughts as well.

Finally, Dr. Geri Richmond is the former Under Secretary for Science and Innovation at the Department of Energy under the Biden Administration. Dr. Richmond currently serves as the Presidential Chair in Science, and is a Professor of Chemistry at the University of Oregon.

Thanks to all three of you for your willingness to appear in front of the Committee. We will now turn to Mr. Dabbar for your opening statement, then to Ms. Puglisi, in order of introduction, and then to Ms. Richmond.

STATEMENT OF HON. PAUL M. DABBAR, CEO AND CO-FOUNDER, BOHR QUANTUM TECHNOLOGY; FORMER UNDER SECRETARY FOR SCIENCE, U.S. DEPARTMENT OF ENERGY

Mr. DABBAR. Chairman Lee, Ranking Member Heinrich, it is great to be in front of this Committee yet again, and seeing many friends here.

America leads the world in discovery and innovation. No one else comes close. One can see that in the Nobel Prizes referenced in the introduction. Examples include nuclear power, generation of chips, fusion, AI, quantum, solar PV, electric vehicles, gene editing, and chemistry of batteries of all types. And much of that was spearheaded at the DOE national labs. But our top adversary, China, puts tremendous pressure in appropriating this innovation and then manufacturing it. Examples include nuclear power stolen from Westinghouse, lithium-ion batteries at CATL, the LFP batteries at BYD stolen from MIT patents, electric vehicles, solar PV, GPUs, semiconductors, and they are trying to steal the future of quantum and fusion.

Let me put this into historical context. When I took over the role of Under Secretary, I discovered that we had significant stealing of technology at the labs. Not only that, but our policy allowed our own researchers to legally be employed by Communist China at the same time as working at our national labs. After finding this out and going through the five stages of grief—I forgot from my academy days that NAVY is an acronym that stands for "never again volunteer yourself"—I started mapping out security policy changes. We banned talent programs. We banned lab employees from working with countries of risk. We created the technology risk matrix to restrict engagement on frontier technologies. We restricted interactions with China and extended Communist China fundraising restrictions on university researchers who got DOE funding. All these felt like bringing back common sense.

However, in the last several years, we have allowed that risk to increase. The Infrastructure Act funding was given to Communist-controlled entities in violation of the Act. As disclosed in the report at the Homeland Security Committee, Communist Chinese nationals who were employed at DOE labs stole inventions in violation of U.S. law, and took them to China for commercialization. They effectively created spy cells by recruiting new members, and they tried to recruit senior lab and former political officials. I wrote about that in the Wall Street Journal, and I submitted that as testimony. We must also remember that all PRC citizens are required by the Chinese National Security Law to hand over all information when directed by the Chinese state.

In addition, DOE has restarted engagement with Communist China in sharing energy technologies. They have been proactively meeting with the Communist government to reestablish transfer of American invention to China. And what was interesting was that this effort was never publicly identified by DOE, but many were able to find that in meetings and articles in local Chinese newspapers, including pictures. And those officials in Communist China were hailing China technology appropriation. I do believe that there are plenty of people who think that this is important to share with Communist China for various different reasons, but I expect

that the majority of the American people do not want us to turn over our technology to our adversaries. And I would venture to say that this is the view of this full Committee.

New controls are needed for science and security, and I know that Secretary Wright is focused on that. While the current DOE orders on the DOE website provide a framework for security and counterintelligence, they provide too much flexibility and discretion for interpretation by politicals, careers, and lab employees. I recommend that the new DOE team roll out significant tightened controls, such as requiring lab under secretaries to be the sole authorizer, with no ability to delegate authority for all countries of risk, nationals hiring, visits by labs or meetings, and also create a list of the waivers that can be found by this Committee for its oversight. The Senate should consider legislation mandating security policies that require administrative policies that politicals would have little discretion in interpreting. I have also included in my written testimony an idea for DOE to recover stolen IP. And the Senate should consider extending the NNSA lab ban on adversary-nation nationals from the three NNSA labs to all the labs.

America is the world's greatest superpower in both technology and in energy. As we invent the future, we should reengage on strong policies to protect our discovery leadership.

[The prepared statement of Mr. Dabbar follows:]

STATEMENT BY

THE HONORABLE PAUL M. DABBAR

FORMER UNDER SECRETARY FOR SCIENCE

U.S. DEPARTMENT OF ENERGY

ADJUNCT SENIOR RESEARCH SCHOLAR, CENTER ON GLOBAL ENERGY POLICY, COLUMBIA UNIVERSITY

CO-FOUNDER, BOHR QUANTUM TECHNOLOGY

BEFORE THE SENATE ENERGY AND NATURAL RESOURCES COMMITTEE

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

FEBRUARY 20, 2025

Chairman Lee, Ranking Member Heinrich, I am honored to again be before this Committee, this time to discuss the current state of technology appropriation risk and security policy at the National Labs.

America leads the world in discovery and innovation. No one else comes close. One can see that in our domination of Nobel Prizes. Examples include nuclear power, new generations of chips, fusion, AI, quantum, solar PV, electric vehicles, gene editing, and batteries of all chemistry types. Much of that is spearheaded by the DOE National Labs.

But our top adversary, communist China, puts tremendous effort into appropriating this invention, and then manufacturing those American inventions. Examples include nuclear power stolen from Westinghouse, lithium-ion batteries at CATL, LFP batteries at BYD, electric vehicles, solar PV, GPU semiconductors, and AI. And they are actively trying to steal the future of quantum and fusion.

Let me put this into historical context. When I took over the role of Under Secretary, I discovered that we had significant spying and stealing of technology at the Labs. Not only that, but that the policy of allowing our own lab researchers to be co-employed by communist China was condoned by DOE. After going through the five stages of grief around the extent of this situation, I forgot from my academy days that NAVY is an acronym for "never again volunteer yourself", I mapped out security policy changes. We banned talent programs, banned lab employees from working for China, created the technology risk matrix to restrict engagement with China on frontier technologies, restricted interactions with China, and extended communist China funding restrictions on university researchers who got DOE funding. All these felt like bringing common sense back for the American taxpayer.

However, in the last several years, we have allowed that risk to increase. Infrastructure Act funding was given to communist controlled entities, in violation of the Act. As disclosed in a report by the Homeland Security Committee, communist Chinese nationals who were employed at DOE labs stole inventions in violation of U.S. law and took them to China for commercialization. They effectively created spy cells by recruiting new members. And they continue to try to recruit senior lab and former political officials. I wrote about that in the Wall Street Journal, that I submitted as testimony. And we must remember that all PRC citizens are required by the Chinese national security law to hand over all information whenever directed, effectively requiring every PRC national to be a spy if directed by the state.

In addition, DOE has restarted engagement with communist China on sharing energy technologies we are inventing at the Labs. Yes you heard me correctly, DOE has been proactively meeting with the communist government to re-establish transfer of the American people's invention to China. And what was interesting about that effort was that it was never publicly identified by DOE in its public affairs. But many were able to find about those meeting from articles and pictures in local

Chinese language newspapers. And those official newspapers were hailing the technology appropriation. My best guess is that there were U.S. officials who believed that the risks of climate change are so important, they needed to engage with our key adversary, including re-starting technology sharing. I also see this world view with certain climate-first advocates. But I know that the vast majority of the American people don't want us to turn over our technology to communist China, and I venture to say I would expect that is also a view of this full committee.

New controls are needed to reassert science security, and I know Secretary Wright is focused on that. While the current DOE orders that are on the DOE website provide a framework for security and counter-intelligence, they provide for too much flexibility and discretion for interpretation by politicals, careers and lab personnel. I recommend the new DOE team roll out significantly tightened controls, such as requiring respective labs Under Secretaries to be the sole authorizer, with no ability to delegate the authority, for all countries of risk nationals hiring at labs, visits by their nationals to labs, or any sort of meeting or engagement with controlled entities or companies. And a list of signed engagement waivers should be publicly posted on the DOE website for proper oversight. The Senate should consider legislation mandating more security policies, to require administration policy that politicals would have little discretion to implement. I have also included in my written testimony an idea for DOE to recover stolen IP. And the Senate should consider extending the NNSA lab ban on PRC nationals at those three labs, to all the labs in the complex.

America has the world's greatest set of strengths to grow our Technology and Energy Superpower status. As we invent the future, we should re-engage on strong policies to protect our discovery leadership.

SUPPLEMENTAL TESTIMONY

BY

THE HONORABLE PAUL M. DABBAR

FORMER UNDER SECRETARY FOR SCIENCE

U.S. DEPARTMENT OF ENERGY

ADJUNCT SENIOR RESEARCH SCHOLAR, CENTER ON GLOBAL ENERGY POLICY, COLUMBIA UNIVERSITY

CO-FOUNDER, BOHR QUANTUM TECHNOLOGY

BEFORE THE SENATE ENERGY AND NATURAL RESOURCES COMMITTEE

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

FEBRUARY 20, 2025

THE WALL STREET JOURNAL.

How the Chinese Communist Party Steals U.S. Technology

A Thousand Talents is 999 too many.

By Paul Dabbar
Aug. 17, 2022 1:46 pm ET

The Idaho National Laboratory's Materials and Fuels Complex, Sept. 9, 2009. PHOTO: HO NEW/REUTERS

When I joined the U.S. Department of Energy in 2017, I was briefed about how pervasively the Chinese Communist Party had woven itself into the U.S. government's research and innovation efforts. Traditionally, labs and academic institutions around the world and their researchers work

on projects together. And periodically, foreign institutions, including in China, compensate Americans for their efforts. The Communist Party began to use these

I should have known. Before I joined the department, I was in the nuclear industry in the private sector, and served on an Energy Department advisory board. Chinese state entities often invited me to attend nuclear conferences and tour the country—all expenses paid. I always said no, because I was too busy. In retrospect, I certainly am glad I was. The invitations have resumed since I left the government, and my answer is a well-informed no.

I learned that people working at the Energy Department's National Laboratories had significant engagements with China. Some were paid by one of the many Chinese Communist Party Thousand Talents Plans while concurrently working at sensitive U.S. government labs. These agreements often required technology transfer as well as support for recruiting more members to the TTPs. This was also happening at other agencies, and it was recently disclosed that these include nonscience and international institutions such as the Federal Reserve and the Inter-American Development Bank.

The weakness in the Energy Department's compliance rules was that there were no disclosure or conflict-of-interest policies regarding foreign engagement or research and technologies other than those involving strategic weapons. There were no rules about research in quantum computing and artificial intelligence, which will have a large economic impact and defense applications.

During my tenure, the department developed and rolled out four orders to restrict China's recruiting and appropriation of innovation. First, mandate disclosure and develop conflict-of-interest policies for department and national-lab employees regarding countries of risk (China, Russia, Iran and North Korea), including a ban on TTP membership. Second, develop a "technology risk matrix," a map detailing which technologies we would collaborate on with those countries, and which we wouldn't. Third, increase oversight on interactions by any program or employee with those countries. Fourth, require that any researcher supported by a department grant (including at U.S. universities) not be a member of a TTP.

A recent report about vanadium battery technology appropriated last year from Energy Department efforts shows there are still significant gaps, but these policies were a good start.

Mr. Dabbar served as undersecretary of energy for science, 2017-21.

THE HILL

How existing laws can help the US recover technology stolen by China

by Paul Dabbar and Ted Garrish, opinion contributors - 02/01/24 8:30 AM

China's President Xi Jinping attends the "Senior Chinese Leader Event" held by the National Committee on US-China Relations and the US-China Business Council on the sidelines of the Asia-Pacific Economic Cooperation (APEC) Leaders' Week in San Francisco, California, on November 15, 2023. (Photo by CARLOS BARRIA/POOL/AFP via Getty Images)

For over a generation, China has been appropriating U.S. technology discovery, building new industries from those new technologies and selling them around the globe, including back to us. Many recent technologies that China leads in, like lithium ion and lithium iron phosphate batteries and photovoltaic solar, were not invented in China. They were mostly discovered in America, supported by significant U.S. government funding.

To a large degree, U.S. counter efforts on China's technology appropriation have been focused on preventing more stealing, and the response to what has been already appropriated has been mostly to

just complain. However, the U.S. government has significant intellectual property and contractual rights to much of that technology due to its financial support of technology research at the early stages.

The U.S. should take action to recover that intellectual property and halt China from selling products in the U.S. and globally that violate those rights. This could significantly repatriate the manufacturing of stolen technology to the U.S. and also prevent China from appropriating and commercializing even more U.S. technology being developed with the assistance of taxpayer funding.

U.S. government agencies provide more than $150 billion in funding per year for discoveries of all types, including those from the Departments of Energy, Defense, Commerce, Health and Human Services, NASA and the National Science Foundation. The government typically has several types of IP and commercialization rights embedded in the grants as a part of that funding.

The largest IP rights bucket is under the terms of the Bayh-Dole and Stevenson-Wydler Acts, which require research recipients to attempt to commercialize any inventions that come from their work, with specific obligations. If the recipients don't execute on those terms, the government has "march-in rights" to reclaim the IP and control how the rights are subsequently licensed.

Any appropriation of IP from labs, universities or companies supported by the U.S. government, from open source or illegal appropriation by the Chinese, is likely in violation of the IP requirements under the acts. And the various government agencies already have authorization to march in on the IP and exert legal rights.

Another common legal requirement of government technology research and development grants is a "build in America" clause. This typically requires that if the technology becomes commercialized, it must be materially built in the U.S. to be sold here.

These and other historical federal funding requirements for many technologies now being sold by China are likely being violated. So instead of wringing our hands and complaining about all that has been stolen by the Chinese, the government should exert its various rights and prevent China from selling those products.

The government could start a China IP Initiative to claw back our discovery commercialization in energy, biotechnology, information technology and other sectors. The respective agencies could identify key technologies that were supported under Bayh-Dole and other authorities, coordinate with the Justice Department, which manages litigation for the departments and take action to secure the IP and enforce its rights globally. It could also possibly work through the Commerce Department and the International Trade Commission to issue Section 337 actions that would prevent those affected products from being sold in the U.S.

In addition, the government could extend its actions to international jurisdictions, like the European Union, whose legal IP protections could likely support our action there too. There are possibly similar IP protections in the European Union, United Kingdom and elsewhere that could also be enforced based on early governed funding in those jurisdictions.

The U.S. government provides significant support for research and development. In doing so it has clear IP rights, and no new legislative authority is needed to act on these material rights. The government should take action with these rights to reclaim and protect the investment from Chinese appropriation.

Paul Dabbar is a former undersecretary for Science at the U.S. Department of Energy and CEO of Bohr Quantum Technology. Ted Garrish served as assistant secretary of international affairs and general

counsel at U.S. Department of Energy and is principal at Annapolis Energy Consulting.

16

Safeguarding the Research Enterprise

Contact: Gordon Long—glong@mitre.org

JSR-23-12

March 21, 2024

JASON
The MITRE Corporation
7515 Colshire Drive
McLean, Virginia 22102
(703) 983-6997

Contents

This Page Intentionally Left Blank

1 EXECUTIVE SUMMARY

The National Science Foundation (NSF) is the premier government organization supporting fundamental scientific and engineering research in the United States. In 2019, NSF asked JASON to comment on how NSF might respond to growing concerns that the openness of the U.S. academic research system was being taken advantage of by other countries. The resulting JASON report, *Fundamental Research Security*, discussed the issues of both research integrity and research security, and identified four major themes:

- The value of, and need for, foreign scientific talent in the United States;
- The significant negative impacts of placing new restrictions on access to the results of fundamental research;
- The need to extend our notion of research integrity to include disclosures of commitments and potential conflicts of interest; and
- The need for a common understanding between academia and U.S. Government agencies about how to best protect U.S. interests in fundamental research while maintaining openness and successfully competing in the global marketplace for science talent.

In the 4 years since the 2019 report, the discussion of how best to address issues of research security has evolved. Legislation, such as the CHIPS and Science Act of August 2022, has further defined NSF's obligations to identify and protect certain types of research—in particular, those involving Controlled Unclassified Information (CUI). In addition, other U.S. government agencies, such as the Department of Energy (DOE) and the Department of Defense (DOD), have developed approaches to identify and mitigate risks to national security from research funded by their organizations. Given the evolving landscape for research security, NSF asked JASON to comment further on specific steps it might take to identify sensitive areas of research and describe processes NSF might use to address security in those research areas of concern.

JASON was asked:

1. What are the general principles that NSF might use in developing lists of research/technology areas of concern?
2. What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?
3. What processes might NSF establish for annually reviewing its list of research/technology areas of concern?
4. Using one or more specific research/technology areas, as examples, what detailed evaluation criteria might NSF use for identifying research/technology areas of concern?
5. What are some of the potential impacts on the research community should some NSF-funded research areas be designated as areas of concern?
6. What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?

In addressing these questions, JASON had frequent discussions with NSF leadership and heard a wide spectrum of ideas from individuals from various government agencies, university administrators, and experts on issues of research security. We came to understand that the subject of *research security* is much broader than the narrower issue of *research controls*, and that there is a need to go beyond research controls toward a broader strategy for enhancing research security for NSF.

Our study endorses the major themes of the 2019 JASON report, and considers the following additional themes.

- Fundamental research is a critical component of U.S. scientific and technical leadership, promoting national security in both defense and economic domains.
- Recipients of federal funding have a responsibility to protect U.S. interests, and the U.S. research community should be actively engaged in protecting those interests.
- Transfers of sensitive technologies to foreign countries can create national security risks.

- Research controls, such as CUI, are only one component of a broader strategy of risk mitigation and management to ensure that U.S. research contributes significantly and positively to the national interest.

Our principal findings and recommendations address and build on these themes, and suggest approaches NSF might use to identify research areas of concern, as well as processes for mitigating the risks to national security in those areas. This report focuses on security for research that has potential military or defense applications, rather than on research with potential economic implications.

JASON presents the following Key Findings and Recommendations.

1.1 Key Findings

1. Openness and transparency in fundamental research promote scientific discovery, which improves national security.

2. International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC.

3. Differentiation between sensitive and non-sensitive research is most natural at the project level, not at the sub-field level. Projects in the same sub-field can have very different levels of risk.

4. Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that benefits outweigh the costs.

5. Formal controls on research, such as a CUI designation, will have unintended consequences, including: increasing the cost of doing research, diverting resources better applied to expanding U.S. research efforts in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research.

6. The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects—i.e., those projects for which the release of information about research execution or outcomes could have a significant, direct, and predictable impact on national security.

7. Research institutions and NSF have key roles to play in the process of risk identification and management. Dialogue between NSF and research institutions such as universities is critical.

8. Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level, and such steps are mandated under the CHIPS and Science Act.

1.2 Key Recommendations

1. NSF should adopt a dynamic approach for identifying potentially sensitive research topics as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas. NSF's process of identifying sensitive research projects should:

   - Differentiate research projects based on the sensitivity of their potential applications,
   - Include the maturity of the development path (Technology Readiness Level—TRL) for potential applications in the assessment of risk, and
   - Include an assessment of the direct and predictable national security impact of the applications of each research proposal, if successful.

2. NSF should proceed with caution before adding access or dissemination controls to grants or contracts. In considering whether to apply formal controls to a sensitive research project, NSF should weigh the balance between the positive protective benefits and the unintended negative consequences of such controls. Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and national security interests.

3. The identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. We recommend that the principal investigator (PI) and the NSF program officer, with guidance from the NSF Division Office, determine if a proposal constitutes a sensitive project. NSF may wish to implement a pilot program within some division of NSF to gain experience with the process. NSF should consult with other federal research funding agencies such

as the Department of Energy (DOE), the National Institutes of Health (NIH), and the Department of Defense (DOD) to help identify sensitive research.

4. Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the sponsored projects office of the institution accepting responsibility for execution of the research. Specific mitigation steps should be proportionate to the assessed risk, relative to the associated costs.

5. NSF should foster a culture of research security awareness by providing substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions about the efficacy of research risk mitigation and control efforts.

6. NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

1.3 Conclusions

This report recommends specific steps that NSF can take to enhance awareness of research security, both within NSF and in the research community. It also suggests mechanisms for NSF to address research projects that are identified as sensitive because of their possible impact on national security. The processes we describe are compatible with the existing NSF structure and its emphasis on funding of research proposals from individual researchers and research organizations. The processes are flexible and adaptable so that they can respond to changing conditions and thinking about research security. While our recommendations focus on academic research security, many are relevant to NSF-funded R&D at organizations other than institutions of higher learning.

This Page Intentionally Left Blank

2 INTRODUCTION AND CONTEXT

2.1 Historical Retrospective: We Have Been Here Before

We are in a period of debate about how to ensure U.S. research security in a manner that does not undermine the great benefits that research in science and technology (S&T) brings to our Nation. In the past few years, policymakers across the U.S. Government have expressed increasing concern that foreign nations, principally the People's Republic of China (PRC), seek to exploit the fruits of U.S. scientific and technological research for purposes that are harmful to U.S. interests.

However, this is not the first time that a national debate has been raised on the issue of research security. In the 1980s, there was concern about Soviet technology acquisition, and it was apparent that the Soviets were making a concerted worldwide effort to secure military technology and know-how.[1] The security concerns extended to new technology early in the R&D cycle by universities and research centers. To help address these concerns, Richard DeLauer, Under Secretary of Defense for Research and Engineering, established a DOD-university forum. DeLauer worked with Frank Press, President of the National Academy of Sciences (NAS), to set up a panel of the NAS, chaired by Dale Corson of Cornell, that included representatives from government, industry, and academia. The panel's mission was to discuss the relationship of scientific research to national security. In September 1982, the Corson panel[2] found that:

> Scientific communication is traditionally open and international in character. Scientific advance depends on worldwide access to all the prior findings in a field—and, often, in seemingly unrelated fields—and on systematic critical review of findings by the world scientific community.

and further found that:

> Controls on scientific communications can be considered in the light of several national objectives. Controls can be seen to strengthen national

[1] Mario Daniels and John Krige, *Knowledge Regulation and National Security in Postwar America*, Chicago, IL: University of Chicago Press, 2022. [1]

[2] National Academies of Sciences, Engineering, and Medicine, Committee on Science, Engineering, and Public Policy, "Scientific Communication and National Security," Washington, DC: National Academies Press, 1982, accessed December 18, 2023, https://doi.org/10.17226/253. [2]

> security by preventing the use of American results to advance Soviet military strength. But they can also be seen to weaken both military and economic capacities by restricting the mutually beneficial interaction of scientific investigators, inhibiting the flow of research results into military and civilian technology, and lessening the capacity of universities to train advanced researchers. Finally, the imposition of such controls may well erode important educational and cultural values.

Finally, in underlined text, the Corson panel concluded that:

> in comparison with other channels of technology transfer, open scientific communication involving the research community does not present a material danger from near-term military implications.

As an interesting nuance, the report stated:

> The Panel found it possible to define three categories of university research. The first, and by far the largest share, are those activities in which the benefits of total openness overshadow their possible near-term military benefits to the Soviet Union. There are also those areas of research for which classification is clearly indicated. Between the two lies a small "gray area" of research activities for which limited restrictions short of classification are appropriate.

Forty years later, we are again discussing possible controls on a "gray area" of research for which limited restrictions short of classification might be appropriate. Our report considers this "gray area" in the current context of the U.S. research enterprise, and specifically how NSF might identify sensitive research projects; and what NSF can do, working with universities and other funded research organizations, to mitigate risks to research security.

The Corson Report was followed in September 1985 by President Ronald Reagan's National Security Decision Directive (NSDD)-189, National Policy on the Transfer of Scientific, Technical and Engineering Information, which referred to the Corson Report and defined fundamental research as follows:

> "Fundamental Research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community.

NSDD-189 continues:

> It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where national security requires control, that the mechanism for control of information generated during federally-funded fundamental research at colleges, universities and laboratories is classification.

The document concluded:

> No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes.

The important question for U.S. research security today is: *Has the situation changed significantly enough that the principles underlying unrestricted fundamental research need to be re-examined?* In this report, we judge that those principles remain valid, but the evolving context of the U.S. research enterprise requires new approaches to ensure research security in cases of substantive perceived risk. Recognizing that restrictions and controls are not the only, or even the most effective, approach to ensure research security, this report explores how best to identify sensitive areas of research and discusses the broad spectrum of responses available to address issues of research security.

2.2 What Has Changed?

Some of the changes affecting security in the U.S. research enterprise include:

- The perception that national defense is increasingly connected to technology innovation in the civilian commercial sector. Examples include large constellations of commercial satellites and the development of artificial intelligence (AI) and large language models by the commercial sector. Supply chain issues are another aspect of this linkage. While a strong economy has long been recognized as essential to a strong national defense, in the past, technologies have often flowed from the military to the civilian sector (e.g., the internet and GPS.) We now see growth in the flow in the opposite direction.

- The increasing connection and decreasing distance between areas of academic research and their application and commercial development. The new NSF Directorate for Technology, Innovation, and Partnerships (TIP), authorized by the CHIPS and Science Act,[3]. is a recognition of this linkage.
- The increasing globalization of the research enterprise, driven in part by the broad dissemination of knowledge via the internet.
- The continuing rise of the PRC as a peer competitor to the United States, together with concerns about the PRC's policies of military–civil fusion.
- The evolving regulatory and legislative landscape in the United States with respect to research security.

As context for this report, we now discuss recent changes in the regulatory and legislative landscape, and the changing situation with respect to the PRC.

2.3 Recent Directives and Legislation

Since the Corson Report in 1982, and NSDD-189 in 1985, additional orders, regulations, and legislation have implications for research security in the United States.

Executive Order 13556: Controlled Unclassified Information (CUI). A 2010 executive order from President Barack Obama[4] stated:

> This order establishes an open and uniform program for managing information that requires safeguarding or dissemination controls... At present, executive departments and agencies (agencies) employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information

[3]U.S. Congress, *CHIPS and Science Act*, 117th Congress (2021–2022), Public Law No. 117-167, 2022, accessed December 18, 2023, https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf

[4]Office of the President of the United States, *Controlled Unclassified Information, Executive Order 13556 of November 4, 2010*, accessed December 18, 2023, https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf.

> sharing... To address these problems, this order establishes a program for managing this information, hereinafter described as Controlled Unclassified Information.

Executive Order 13556 established the concept of CUI and declared the National Archives as being the responsible organization for implementation and oversight of the actions of federal agencies regarding CUI. The implementing regulation for CUI was stated later, in 2016, in the Code of Federal Regulations (CFR).[5] While Executive Order 13556 makes no mention of research security itself, CUI is part of the implementation guidelines for both National Security Presidential Memorandum (NSPM)-33 and the CHIPS and Science Act, described next.

National Security Presidential Memorandum (NSPM-33). In January 2021, the broader issues of security for government-supported R&D were addressed in NSPM-33[6] at the end of the Trump Administration. In January 2022, the National Science and Technology Council (NSTC) issued guidance for implementing NSPM-33,[7] which provided further details on how federal agencies should implement the provisions of NSPM-33. Together, these two documents describe the executive branch guidelines for funding agencies and funded organizations regarding research security. Additionally, a "Draft Research Security Programs Standard Requirement"[8] was circulated for public comment by the NSTC in February 2023. This document discussed draft guidelines for universities and other research organizations in several areas, including training, travel, and disclosures.

[5]"Controlled Unclassified Information (CUI)," *Code of Federal Regulations*, title 32 (2018): 497–517, accessed December 18, 2023, https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf.

[6]Office of the President of the United States, *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, (January 14, 2021), accessed December 18, 2023, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/.

[7]NSTC, Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*, 2022, accessed December 18, 2023, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf. [3]

[8]NSTC, Office of Science and Technology Policy, Subcommittee on Research Security, *Draft Research Security Programs Standard Requirement*, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf [4], accessed December 18, 2023.

CHIPS and Science Act. August 2022 saw passage of the landmark CHIPS and Science Act,[9] which describes the detailed provisions for individual federal agencies regarding research security, including the Department of Energy (DOE) and NSF. In particular, Title III, Subtitle D of the CHIPS and Science Act is named "NSF Research Security," and a few selected sections include: establishment of an Office of Research Security and Policy within the NSF Director's Office, NSF development of online resources describing NSF research security policies and best practices for mitigating security risks, training for academic researchers in research security, establishment of a research security and integrity information sharing analysis organization (RSI-ISAO), and ensuring proper protections for CUI. The CHIPS and Science Act also calls for establishment of the NSF TIP Directorate. In addition to agency-specific guidance on research security, the law mandates research security training for federal research award personnel. A useful summary of research security provisions of the CHIPS and Science Act has been provided by the American Association of Universities (AAU).[10]

Taken together, Executive Order 13556, NSPM-33, and the CHIPS and Science Act form the basis of federal guidance with respect to research security.

2.4 The Changing Situation vis-à-vis the PRC

Much of the current discussion on research security has been prompted by the rise of the PRC as a peer competitor to the United States in S&T. Competition between nations is not new, and can even be constructive; what is of concern is the PRC's widespread acquisition of U.S. technology through duplicitous or illegal means.[5] As of the writing of this report, the Biden Administration has adopted a "small yard, high fence" approach,[11] enacting targeted trade restrictions on selected critical technology

[9] U.S. Congress, *CHIPS and Science Act*, 117th Congress (2021-2022), Public Law No. 117-167, 2022, accessed December 18, 2023, https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf.

[10] AAU, *The CHIPS and Science Act of 2022 (H.R. 4346) Research Security Provisions*, August 8, 2022, accessed December 18, 2023, https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf.

[11] The White House, "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Policy," October 12, 2022, accessed December 18, 2023, https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy. [6]

areas.[12] This JASON report does not focus on economic and trade issues, but rather on the issue of research security in key areas of S&T with implications for national defense.

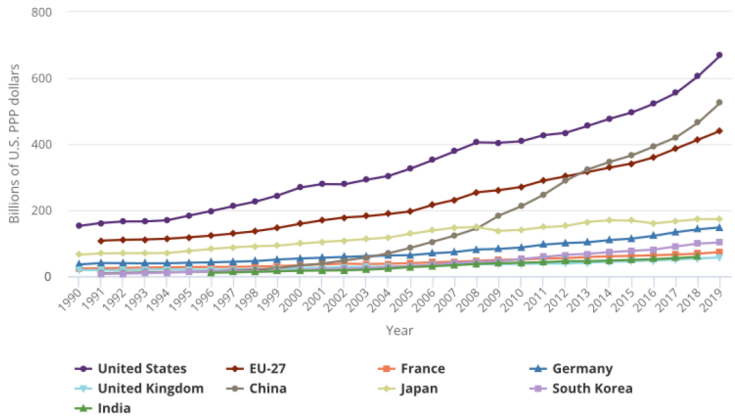

Figure 1: Gross domestic expenditures on R&D, by selected region, country, or economy: 1990–2019. The expenditures are adjusted for purchasing power parity (PPP).

The PRC as a Peer Competitor in R&D.
Figure 1 shows the R&D expenditures for the United States, the PRC, the European Union (EU), and several other countries between 1990 and 2019.[13] The figure clearly shows a sharp increase in R&D investment by the PRC relative to the United States. It also shows that the combined U.S. and EU investment is more than twice that of the PRC, as of 2019 (note that 2019 was prior to the Covid-19 pandemic).

The PRC's government funding for higher education more than doubled over the last decade. When adjusted for purchasing power parity (PPP), Ministry of Education

[12]The White House, "President Biden Signs Executive Order on Addressing United States Investments In Certain National Security Technologies And Products In Countries Of Concern," (August 09, 2023), accessed December 18, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/president-biden-signs-executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern. [7]

[13]NSF, National Science Board (NSB), *Science and Engineering Indicators*, 2022, *Research and Development: U.S. Trends and International Comparisons, NSB 2022-5*, (April 28, 2022), accessed December 18, 2023, https://ncses.nsf.gov/pubs/nsb20225. [8]

(MOE) spending on higher education now exceeds $179 billion.[14] Perhaps as a result of these efforts, the PRC has surpassed the United States in publishing the largest number of scholarly papers annually.[15]

The PRC's global position in research is clearly a major priority, and the PRC is investing in targeted areas identified as critical emerging technologies.

Another key statistic with significant long-term implications for R&D leadership is the total number of STEM (science, technology, engineering, and mathematics) PhDs educated in the United States compared to the PRC; and further, the number of domestic PhDs educated in the United States, shown in Figure 2.

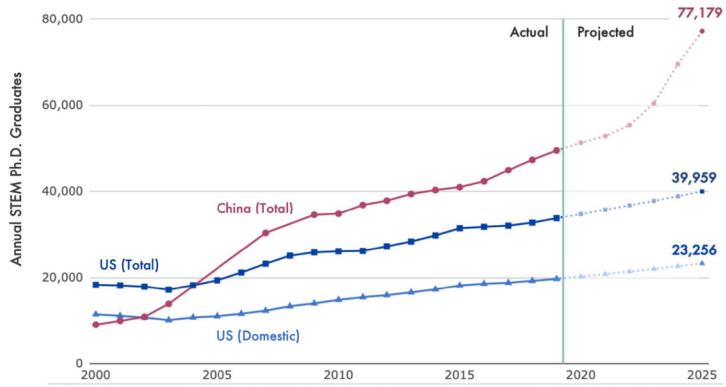

Figure 2: The number of STEM PhD graduates in the PRC has rapidly outpaced the United States in the last 20 years. Regarding the projections, the authors of the report in which the figure appears explain: "The Chinese Ministry of Education publishes data on the number of students who enter PhD programs each year. In recent years, for every 100 students who enter a Chinese STEM PhD program, an average of 93 students obtains a PhD six years later... The rapid growth in projected graduates after 2022 is due to rapid growth in PhD entrants after 2016."[16]

[14]Ryan Fedasiuk et al., "A Competitive Era for China's Universities: How Increased Funding Is Paving the Way," *Center for Security and Emerging Technology (CSET)*, (2022), accessed December 18, 2023, https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf. [9]

[15]NSF, NSB, *Science and Engineering Indicators 2022, Publications Output: U.S. Trends and International Comparisons, NSB-2021-4*, October 28, 2021, accessed December 18, 2023, https://ncses.nsf.gov/pubs/nsb20214/international-collaboration-and-citations. [10]

Figures 1 and 2 together indicate that the PRC is domestically producing significantly more STEM PhDs than the United States, and significantly more STEM PhDs per dollar invested in domestic R&D than the United States. While a significant fraction of the U.S. R&D effort is carried out by individuals with degrees other than a PhD, the trends are consistent with the view that the United States has challenges in building a large STEM labor force[17] and that the size of the skilled U.S. STEM labor force may hamper its R&D growth in the future.

Finally, Figure 3 indicates a falloff in the number of students from the PRC studying in the United States. This may be due to several factors, including a perception that the United States is not entirely welcoming to Chinese students, or the difficulty PRC students face acquiring visas for study in the United States. While the pandemic likely also has been a factor, Figure 3 indicates that the total number of international students in the United States has rebounded from its post-Covid minimum, in contrast to the number of students from the PRC, which remains below pre-pandemic numbers. This may be a further indication that the PRC is shifting its incentives and priorities more toward domestic training of graduate students and away from training at institutions outside the PRC.

To maintain leadership in critical technology areas, the United States will need to invest significantly in its own targeted R&D efforts and in the development of its broad STEM workforce. While it is expected that the PRC will continue to attempt to exploit the results of U.S. R&D for its economic and military benefit, it should be clear that *protection of U.S. research from such exploitation will be insufficient by itself to ensure U.S. leadership in critical technologies.* As the PRC increases its competitiveness with the United States in R&D, the PRC's own internal domestic R&D will increasingly power its economic and military development.

The PRC's Military–Civil Fusion (MCF).
The PRC's MCF is a government-led program meant to leverage all state, academic, and commercial developments to strengthen the PRC military. Specifically, it aims

[16]Remco Zwetsloot et al., "China is Fast Outpacing U.S. STEM PhD Growth," *Center for Security and Emerging Technology (CSET)*, (2021), accessed December 18, 2023, https://doi.org/10.51593/20210018. [11]

[17]NSF, NSB, *Science and Engineering Indicators 2022, The State of U.S. Science and Engineering 2022, NSB-2022-1, Conclusion*, accessed December 18, 2023, https://ncses.nsf.gov/pubs/nsb20221/conclusion. [12]

[18]The Open Doors Report on International Educational Exchange is a comprehensive information resource on international students in the United States and U.S. students studying abroad. It is sponsored by the U.S. Department of State, with funding provided by the U.S. Government, and is published by the Institute of International Education. See https://opendoorsdata.org/data/international-students/leading-places-of-origin/ (accessed December 18, 2023).

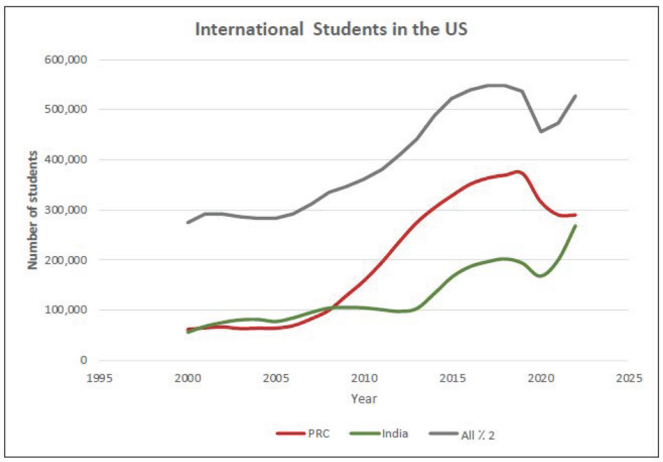

Figure 3: U.S. Department of State data suggest that the number of students from the PRC studying in the United States leveled off prior to the 2020 start of the Covid-19 pandemic, then dropped precipitously, and has not returned to pre-pandemic levels. This is in contrast to the total number of international students in the United States, which has rebounded to pre-pandemic levels, as well as the number of students from India, which is growing dramatically and now exceeds pre-pandemic levels. The PRC and India are the countries with the largest numbers of students in the United States. Note that the curve for the number of students from all countries has been reduced by a factor of two for presentation purposes.[18]

to "Establish a complete policy and institutional system for S&T military–civil fusion. Basically build a policy and institutional system for military–civil fusion with complete systems, linked support, and effective incentives, issue a series of supporting policies to promote S&T military–civil fusion in terms of fiscal spending, prices, investment, financing, and S&T awards, promote the further optimization of the policy and institutional environment for military–civil fusion, and facilitate the flow of innovative elements for S&T military–civil fusion."[19]

The PRC's MCF is significantly different from Civil–Military Integration (CMI) in the United States (see, e.g., [14]). Both have the goal of ensuring that innovations in the civilian sector are utilized effectively by the military. However, while the government

[19]PRC Ministry of Science and Technology (MOST), The "13th Five-Year Special Plan for S&T Military–Civil Fusion Development," June 24, 2020, accessed December 18, 2023, https://cset.georgetown.edu/publication/the-13th-five-year-special-plan-for-st-military-civil-fusion-development/. [13]

of the PRC plays the central role in MCF, mandating and directing fusion activities in the civilian sector, the U.S. approach is decentralized and depends on voluntary cooperation between the U.S. civilian and military sectors, using mechanisms such as research grants and technology-sharing agreements.

The PRC is systematically reorganizing both Chinese academic and industrial enterprises to maximize simultaneous economic and military development. MCF focuses on emerging technologies, specifically "Artificial Intelligence, bio-tech, advanced electronics, quantum, advanced energy, advanced manufacturing, future networks, [and] new materials," in order "to capture commanding heights of international competition."[20] While the PRC term for MCF is not used explicitly in the 14th Five-Year Plan, the plan describes deepening of military–civilian S&T collaboration and adds maritime, aerospace, cyberspace, biotech, and AI to the list of areas for military–civilian development activities.[21]

The ability of the PRC to direct research toward specific targeted areas, and its willingness to close off the external flow of basic scientific information,[22] represents an extreme asymmetry with the global trend to support a broad base of scientific R&D together with open access to scientific data. Further, the PRC's MCF plans allow the ability to direct a vast set of resources (in terms of both civil R&D workforce and capital) toward targeted areas, so as to dwarf U.S. investments that are more broadly based and more open. The U.S. approach to open collaboration and open, broad dissemination of not just results, but also raw data, has contributed to accelerated innovation within the United States and to the efficient leveraging of the results of fundamental research. Further, the potential for fundamental research to result in impactful innovation has been vital in creating the U.S. technology base. As a result, it is hard to predict the long-term implications of the PRC's "closed and directed" MCF policy.

After considerable research and deliberations, JASON arrived at the following finding.

[20]Richard A. Bitzinger, "China's Shift from Civil-Military Integration to Military-Civil Fusion." *Asia Policy* 16, no. 1 (2021): 5-24, https://doi.org/10.1353/asp.2021.0001 (accessed December 18, 2023). [15]

[21]PRC, Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035[中华人民共和国国民经济和社会发展第十四个五年规划和 2035 [年远景目标纲要], Xinhua News Agency [(新华社)], March 12, 2021. Chinese source text: https://perma.cc/73AK-BUW2, translation: https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf (accessed December 18, 2023). [16]

[22]Beginning in Fall 2022, the Cyberspace Administration of China began implementing regulations that require the review of major exports of data; and in April 2023, the China National Knowledge Infrastructure platform cut 1,600 institutional users outside mainland China from access to some of its database of statistical and academic publications. See https://www.scmp.com/news/china/article/3214808/portal-china-closing-least-temporarily-and-researchers-are-nervous (accessed December 18, 2023).

> **Finding:** International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC.

While research security to protect against the potential that a foreign actor may misappropriate U.S. R&D efforts is of significant concern, future technological threats may arise from the asymmetrical strategies for the development of critical and emerging technologies in the PRC versus the United States. This future threat is likely best addressed by maintaining or establishing U.S. scientific leadership in critical emerging areas, particularly those that are fundamental, with potential for long-term impact.

2.5 Prior JASON Guidance on Research Security

The 2019 JASON report, *Fundamental Research Security*,[23] provides important context for the current report. We therefore summarize the most relevant findings and recommendations of the 2019 report here and provide its Executive Summary in full in Appendix B.

The 2019 JASON report found that foreign-born scientists and engineers training and working in the United States have made essential contributions to our country's preeminence in science, engineering, and technology; and maintaining that leading position will require that the United States continues to attract and retain the best science talent from around the world. Furthermore, NSDD-189, National Policy on the Transfer of Scientific, Technical and Engineering Information, remains a cornerstone to the fundamental research enterprise that protects the free exchange of ideas.

The 2019 report found that concern over actions of the government and institutions of the PRC that are not in accord with U.S. values of scientific ethics is justified. There are credible problems with respect to research transparency, lack of reciprocity in collaborations and consortia, and reporting of commitments and potential conflicts of interest related to these actions. Exacerbating the issue, U.S. academic leadership, faculty, and front-line government agencies lack a common understanding of undue foreign influence in U.S. fundamental research, the possible risks it poses, and the

[23]Gordon Long, "JSR-19-2I Fundamental Research Security," MITRE Corporation (2019), accessed December 18, 2023, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf. [17]

potential detrimental effects that might result from restrictions on such research. Universities and research funding agencies have policies and guidelines regarding some of these responsibilities, but these are often insufficient for individuals to assess risk and take appropriate actions.

JASON recommendations to address the concerns were based on principles of openness, communication, and engagement with stakeholders. The 2019 report recommended that NSF support reaffirmation of the principles of NSDD-189, which make clear that fundamental research should remain unrestricted to the fullest extent possible. It recommended that NSF take lead in working with NSF-funded universities and other entities, as well as professional societies and publishers, to ensure that the responsibilities of all stakeholders in maintaining research integrity are clearly stated, acknowledged, and adopted. JASON furthermore recommended that NSF engage with intelligence agencies and law enforcement to communicate to academic leadership and faculty the scale and scope of risks posed by foreign influence in fundamental research, while also communicating to other government agencies the critical importance of foreign researchers and collaborations to U.S. fundamental research. An additional recommendation was that NSF further engage with the community of foreign researchers in the United States to enlist them in the effort to foster openness and transparency in fundamental research, nationally and globally, as well as to benefit from their connections to identify, recruit, and retain the best scientific talent.

Regarding CUI, the 2019 report found that while the designation in existing categories (HIPAA, FERPA, export control, and Title XIII) is suitable in the relevant circumstances, it is ill-suited to the protection of fundamental research areas. JASON specifically discouraged the designation of new CUI definitions as a mechanism to erect intermediate-level boundaries around fundamental research areas. Based on evolving circumstances, described in Section 2.2, the current report revisits in detail this topic.

Another JASON report, from 2022, *Research Program on Research Security* (JSR 22-08), advised NSF on development of an NSF-funded program on research security. The 2022 report reaffirmed the need to keep the United States a premier destination for international scholars, as well as the necessity for communication and coordination among government agency and academic stakeholders.

2.6 Guiding Themes for the Current JASON Report

The current report endorses the major findings of the 2019 and 2022 JASON reports, and highlights the following themes, which helped guide the deliberations described in the remainder of this report.

- Fundamental research is a critical component of U.S. scientific and technical leadership, promoting national security in both defense and economic domains.
- Openness and transparency, with appropriate controls, are essential in fundamental research, both to validate results and to promote discovery.
- Recipients of federal funding have a responsibility to protect U.S. interests, and the U.S. research community should be actively engaged in protecting those interests.
- Transfers of sensitive technologies to foreign countries can create U.S. national security risks.
- Research controls are only one component of a broader strategy of risk mitigation and management to ensure that U.S. research contributes significantly and positively to the national interest.

3 DEFINITIONS

In writing this report, we became aware of the need to formulate definitions of important words and phrases, as terms like "research" have different meanings depending on the specific context in which they appear. For clarity, throughout this report, we use the working definitions provided in this section.

We first define the related concepts of *national security* and *research security*. We then define various types of research and the important concept of the *fundamental research exclusion* (FRE). We conclude by providing working definitions of *mitigations* and various categories of *controls*.

National Security
Broadly defined, *national security* implies the protection of the United States, its citizens, and its interests, at home and abroad, from threats. In this report, we specifically deal with threats resulting from the misappropriation of the results of U.S. R&D.

Research Security
We use the definition from the National Science and Technology Council (NSTC) *Guidance for Implementing National Security Presidential Memorandum (NSPM-33)*,[24] "Research security is safeguarding the research enterprise against behaviors aimed at misappropriating R&D to the detriment of national or economic security, related violations of research integrity, and foreign government interference."

Research and Development (R&D)
As defined in the guidance for implementing NSPM-33,

> R&D includes basic research, applied research, and experimental development. *Basic research* is experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts. *Applied research* is original investigation undertaken in order to acquire new knowledge, and directed primarily towards a specific practical aim or objective. *Experimental development* is creative and systematic work, drawing on knowledge gained from research

[24] NSTC, Subcommittee on Research Security, Joint Committee on the Research Environment, *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) On National Security Strategy for United States Government-Supported Research and Development*, 2022, accessed December 18, 2023, https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf. [3]

> and practical experience, which is directed at producing new products or processes or improving existing products or processes.

For conciseness, we define *research* as encompassing all NSF-funded R&D.

Fundamental Research
As defined by National Security Decision Directive (NSDD)-189, *fundamental research* is basic and applied research in science and engineering, the results of which are ordinarily published and shared broadly within the scientific community. Federally funded development work is not formally considered fundamental research as defined by NSDD-189.

Fundamental Research Exclusion (FRE)
The FRE provides that research for which no publication, dissemination, or access restrictions have been accepted is excluded from export control regulations. The exclusion is voided if publication approval is required by the sponsor or the government, or if citizenship-based restrictions have been accepted. The relevant export regulations include Export Administration Regulations (EAR), 15 Code of Federal Regulations (CFR) 734.8(c), and International Traffic in Arms Regulations (ITAR), 22 CFR 120.34(a)(8).

Sensitive and Highly Sensitive Research
A research project is considered *sensitive* if the evolution of the research could feasibly lead to a direct and predictable impact on national security in the future. Research is defined as *highly sensitive* when the release of information about the performance or outcomes can currently be shown to have a significant, direct, and predictable impact on national security. The dividing line between *sensitive* and *highly sensitive* is the difference between the *possibility* of a future impact on national security and the *certainty* of a direct and predictable impact on national security. This is a critical distinction, and it underlies much of the discussion in later sections of this report.

Mitigations
In the context of this report, *mitigations* are any actions taken in the conduct of sensitive research to reduce possible risk to national security. We often use the term *mitigations* to describe actions that do not involve explicit *controls* (see definition for controls).

Controls
In this report, we define *controls* to mean any restrictions on the dissemination of information about performance or outcomes of highly sensitive research. This includes both Controlled Unclassified Information (CUI) and classification, but it can include

restrictions that fall into neither of these categories. Research that requires controls no longer falls within the fundamental research category protected by the FRE (see Section 3.1).

Controlled Unclassified Information (CUI)
The federal directive on implementing CUI (32 CFR 2002) defines CUI as including all unclassified information throughout the executive branch that requires any safeguarding or dissemination control by law, regulation, or government-wide policy.[25] CUI is discussed in detail in Appendix D.

Classification
The system for classification of national security information and for handling of classified information is prescribed in Executive Order 13526. Classification is the most stringent form of control.

3.1 Interrelationships among Definitions

The previous section provided definitions in a form that can be consulted when reading other sections of this report. However, several of the defined terms are interrelated. In this section, we discuss some of those interrelationships.

Sensitive Research and Highly Sensitive Research. *Sensitive research* is research that could likely evolve to have a direct and predictable impact on national security, *but it is not yet sufficiently advanced to know what level of impact it might have in the future.* For this type of research, some degree of risk mitigation is appropriate, but not necessarily formal controls. This research would retain the FRE (see discussion of the FRE later in this section). In contrast, *highly sensitive research* is research that can already be shown to have a direct and predictable impact on national security. For this type of research, formal controls are appropriate. CUI is one type of control, but there are others that may be better suited (see Section 5.1). These formal controls, sometimes referred to as restrictions, void the FRE, with important consequences for researchers.

[25]Note that some categories of information designated as CUI are not sensitive, according to our narrow working definition of sensitivity, which is based on national security impact. However, information in such categories is not relevant to the subject of this report.

Fundamental Research and the Fundamental Research Exclusion. The FRE protects researchers from unintentional export-control violations, allowing researchers to interact and collaborate with, participate in seminars involving, and engage in casual discussions with foreign persons. Critically, these protections allow researchers to publish without obtaining an export license. However, the protections are fragile, and are lost if restrictions are placed on research.

Specifically, the FRE is codified by 22 CFR 120.34(a)(8) and 15 CFR 734.8(c).

The first of these pertains to ITAR restrictions administered by the Department of State, which specify:

> Fundamental research is defined to mean basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if:
>
> (i) The University or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity; or
>
> (ii) The research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

The second of these pertains to EAR restrictions administered by the Department of Commerce. These state:

> Fundamental research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions[26] for proprietary or national security reasons.

[26] Per this section of the code, pre-publication reviews done to ensure the protection of patent rights or to prevent inadvertent disclosure of proprietary information do not constitute a restriction.

In the United States, the communication of protected technology or software to a foreign national in the United States is deemed to be an export[27] and is a crime under the ITAR and EAR. Here, *technology* is very broadly defined as information[28] necessary for the development, production, or even simply the use of a protected product. Because university researchers routinely interact with foreign nationals in laboratories, classrooms, seminars, and conferences, the risk of an inadvertent export is high. In addition, the loss of the FRE would shut down the free exchange of ideas that is an essential component of the training of scientists. Given these serious consequences, actions that would eliminate the FRE should only be used in cases where the research is deemed *highly sensitive*.

National Security and Economic Security. The NSTC definition of *research security* given above refers to the misappropriation of R&D "to the detriment of national or economic security." In this JASON report, we have addressed the *national defense* aspects of research security, where we have taken national defense to include, for example, research areas identified as important by those federal agencies[29] that address military, intelligence, counterterrorism, space, critical infrastructure, or other aspects of national defense. Our guidance in this report on when and how to apply security-related mitigations and controls to research is limited to national defense and does not necessarily extend to the assessment of economic security.

Clearly, NSF-funded R&D can also be of economic importance. While we did not address economic security per se, a significant fraction of our discussion in Section 4 is relevant to economic assessments, including the life cycle of technology development and the assessment of Technology Readiness Level (TRL).

[27]The term "deemed export" is defined in 15 CFR 734.13 as "Releasing or otherwise transferring *Technology* or source code (but not object code) to a foreign person in the United States." For ITAR, 22 CFR 120.50(a)(2) defines an export to include "Releasing or otherwise transferring technical data to a foreign person in the United States," including, by §120.56(a), "(1) Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; (2) Oral or written exchanges with foreign persons of technical data in the United States or abroad; (3) The use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or (4) The use of access information to cause technical data outside of the United States to be in unencrypted form."

[28]The legal definition expressly includes plans, diagrams, models, formulae, tables, specifications, manuals, instructions, skill training, working knowledge, consulting services, etc.

[29]See the NSF Statement of Work (SOW) in Appendix A, which refers to congressional guidance asking "NSF to collaborate with the Secretary of Defense and the Director of National Intelligence to compile and maintain a list of all NSF-funded open source research capabilities that are known or suspected to have an impact on foreign military operations."

This Page Intentionally Left Blank

4 IDENTIFICATION OF SENSITIVE RESEARCH

JASON defines *sensitive research* to mean research for which the release of information about the performance or outcomes could lead to a significant, direct, and predictable impact on national security (see Section 3 for the precise definition). NSF asked JASON to provide guidance on how to identify sensitive research, including specifically whether the existing guidelines for Controlled Unclassified Information (CUI) provide any useful direction. JASON also reviewed a similar identification effort currently underway at the Department of Energy (DOE). Here, we review these existing programs and then share observations about how basic and applied research eventually generate sensitive technology. From this we lay out guidelines for how NSF might identify sensitive technologies at the right stage in their development so as not to unduly harm U.S. technical competitiveness and national security.

4.1 Existing CUI Categories as a Basis for Identifying Sensitive Technologies

The federal regulations regarding CUI are stated in 32 Code of Federal Regulations (CFR) 2002.[30] As a general matter, these regulations dictate data protections but do not identify types of information that need protection. We considered whether any CUI categories defined elsewhere in law or regulation might themselves bring insight. The National Archives' *CUI Registry* gives the complete list of information categories protectable as CUI. JASON reviewed these but did not identify any existing categories that would give NSF useful guidance. For instance, the category of Specified Controlled Technical Information (CUI//SP-CTI)[31] indicates that it includes "research, studies, and analyses with military or space application," but the registry itself does not provide guidance on how to identify which research might be of concern. We note that the SP-CTI category is not limited to the DOD and could apply to research funded by other agencies, such as NSF. However, documents[32] that attempt to describe SP-CTI within the DOD context do not provide relevant guidance to NSF on what might fall under SP-CTI. More detail about CUI and its utility to NSF can be found in Appendix D. Our finding below responds to Question 2 in the Statement of Work (SOW)—see Appendix A.

[30] 32 CFR Part 2002 - Controlled Unclassified Information (CUI), accessed December 20, 2023, https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002.

[31] National Archives, "CUI Category: Controlled Technical Information," Archives.gov, accessed December 20, 2023, https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html.

[32] 48 CFR 252.204–7012, DOD Instruction 3200.12, and DOD Manual 5200.001 Version 4.

Finding: The existing categories of Controlled Unclassified Information (CUI) do not provide useful guidance for identifying sensitive research that might be funded by NSF. The CUI guidelines themselves are silent as to what kinds of information need protecting.

4.2 Insights from the Department of Energy

During its study, JASON heard from both the DOD and the DOE concerning their approaches to research security for unclassified research. The DOD policy for risk-based security reviews emphasizes identifying any association of individual principal investigators (PIs) with foreign entities of concern, while the DOE approach emphasizes the identification of critical research areas. We discuss both approaches in Appendix C. Here, we summarize DOE's process for identifying critical technology areas.

Since December 2018, the DOE has been maintaining a matrix of critical technologies associated with economic competitiveness, national security, and scientific leadership. The DOE approach was developed to protect research carried out within the national laboratory system.

Because the national laboratories are already equipped with an extensive security apparatus, the relative cost of implementing additional protections will be lower than for other research institutions. Nevertheless, the DOE's Science and Technology Risk Matrix effort has proven to be a significant undertaking. After being briefed by the DOE on its effort, we concluded that the task of building and maintaining a predetermined list of sensitive technologies in the DOE fashion is possible mainly because each of the national laboratories has a strong DOE-funded research security organization. The workforce needed to create protection guides in broad areas of unclassified science, and to maintain those guides on a regular basis, appears to be similar to the effort needed to define and maintain classification guides. The DOE has such infrastructure as part of its national laboratories. NSF does not.

A consequence of using broad, list-based categories is that the guidance will remain, by necessity, at least somewhat ambiguous. Small changes to the way a research project is presented can influence how it is categorized. For example, some areas of inquiry can be framed as either robotics research or AI research. In one framing, the project is subject to additional controls under the DOE guidelines; and in the other, it is not. Furthermore, the research in broad categories such as "robotics" and "AI" are likely to include large numbers of projects that present no research security risk. This demonstrates the inherent challenge of attempting to pre-organize large swaths

of science and engineering into a neat tree of knowledge, which is a problem that could be avoided by evaluating technologies as they are being developed, instead of depending on predetermined lists. More detail about the DOE program is available in Appendix C.

> **Finding:** The Department of Energy (DOE) approach involves identifying specific critical areas of emerging technologies and utilizing subject matter experts in evaluating the sensitivity of the research. Regular updating and implementation of this scheme is labor intensive.

4.3 How Are Technologies Created?

For all eventually realized technologies—sensitive and otherwise—there is first an incubation period in which insights and knowledge rooted in basic research grow. This is followed by one or more takeoff periods in which early expectations are tested and, if promising, developed into *application concepts*. If the application concepts are promising, this is followed by a maturation period during which it takes significantly more work to render each application concept into a practical technology.

This sequence can be presented as an "S-curve"[33] (see Figure 4). In the fundamental research stages, open conversation is of significant value. First, the design and testing of each proposed application crucially depends on a community effort to scrutinize the idea's potential, identify shortcomings, and recognize deal-breakers that would ultimately limit the concept's viability. As a result, there are innumerable nascent technologies that were initially hoped to be on a fast trajectory to maturation but for which development efforts pivoted away following open discussion. Second, open research catalyzes other innovations that may ultimately have significant impact of their own. Such innovations can cause seemingly unrelated and mature technologies to be reinvented long after the original concept was considered to have reached maturity. For example, the invention of multi-touch technologies inspired the reinvention of the telephone into the smartphone. Initially, new technologies often underperform, compared to incumbent technologies, but ultimately chart their own independent curve that overtakes the incumbent technology due to improved functionality. This web of innovation depends critically on the free sharing of ideas.

As a result of this disruptive process, a basic-science effort (as is routinely funded by NSF) may spawn many unforeseen application concepts. Equally, real-world chal-

[33]Richard N. Foster, "Working The S-Curve: Assessing Technological Threats," *Research Management* 29, no. 4, (1986): 17-20, DOI: 10.1080/00345334.1986.11756976. [18]

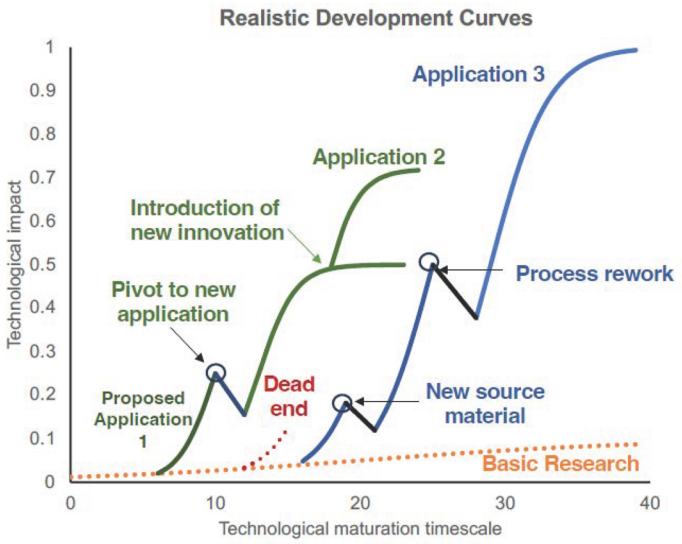

Figure 4: Basic science programs are likely to incubate and then support the takeoff of a number of applications of varying unpredictable growth curves and impact areas, typically illustrated as S-curves. Realistic technological impact curves are discontinuous and illustrate the importance of techno-economic factors on the translation of research concepts into applications. Early-stage exploration will spawn many application concepts, with variable potential impacts. Each concept will in turn be tested for technical success, as well as practical factors such as market scale, cost, supply chain, scale-up, and production feasibility. As concepts evolve, most will fail or pivot to a new application at some stage of development. These curves are rarely continuous, as impediments must be faced and overcome (black lines). Occasionally, new insights catalyze acceleration (or deceleration, as illustrated by varying takeoff points).

lenges can force pivots and reinventions away from the originally envisaged concept. These are notionally illustrated in Figure 4 as S-curves of different colors taking off from a single basic research trajectory. Many concepts fail (represented by a curve that ends abruptly), frequently subsequent to open discussion in the scientific community. Other concepts pause, backtrack, or pivot to a new or modified application at some stage of development, as hurdles are faced and overcome (represented by discontinuities in each of the curves). The timeline for overcoming such hurdles is unpredictable and may take weeks or decades.

For a real-world example in a research area that includes national security–sensitive

technologies, consider the basic science associated with directing the propagation of electromagnetic energy through materials (akin to the orange line in Figure 4). This fundamental research area has spawned many application concepts, such as electromagnetic bandgap structures in split-ring resonators for RF/microwave application, and optical-fiber waveguides. Some were readily successful, such as fiber-optic telecommunications (akin to the green curve). However, other early concepts ran into scaling and manufacturing concerns. The use of metastructured materials for invisibility cloaks[34] is one such example. Had it worked, it would have had obvious national security applications. While macroscopic invisibility cloaks proved unfeasible, such research nevertheless contributed to the foundation (orange line) on which still other technologies of great significance were ultimately realized[35]: the computational packages and patterning schemes needed to form negative-refractive-index materials for invisibility cloaks helped propel the development of metastructured antennae that allowed for effective phase compensation in 5G cellphone radios. The essential insight here is that the premature sequestering of research into a closed setting can significantly slow the development of valuable technologies while also permitting nonviable concepts to persist and consume economic resources longer than they should—both effects that have a negative impact on national security. In relation to Question 5 of the SOW (see Appendix A), this last insight provides a compelling example of the potential negative consequences of unwise decisions regarding research controls.

As technologies become more refined, the work done in support of those refinements becomes increasingly application specific. For many national security–sensitive technologies, a point eventually comes where the balance shifts in favor of protecting those developments because their less-fundamental nature means fewer opportunities to spawn new application concepts in unrelated spaces. Identification of research occurring in these late stages can be facilitated using the well-established framework of Technology Readiness Levels (TRLs).

> **Finding:** At early stages of research, the potential applications' outcomes are notional. Most commonly, highly ambitious potential applications postulated for early-stage research are later replaced with different potential applications, addressing a range of societal, commercial, and national security needs as the research area progresses in technical maturity.

[34] Tolga Ergin et al., "Three-Dimensional Invisibility Cloak at Optical Wavelengths," *Science* 328, no. 5976, (2018): 337-339, accessed December 20, 2023, https://www.science.org/doi/10.1126/science.1186351. [19]

[35] Josh Jacobs, "'Invisibility Cloak' Metamaterials Make Their Way Into Products," *Financial Times*, (2018), accessed December 21, 2023, https://www.ft.com/content/c6864c76-de7d-11e7-a0d4-0944c5f49e46. [20]

4.4 The Utility of Technology Readiness Levels

Technology maturity can be quantified using the framework of TRLs, which can be helpful for guiding NSF in identifying when a concept has reached a state of maturity such that the balance of considerations suggests that national security might be better served by imposing extra mitigations and controls than by maintaining openness. For NSF's purposes, a broad, domain-neutral scheme is needed. For illustrative purposes, we adopted the scheme shown in Table 1.[36]

Technology Development Stage	TRL	Definition
Fundamental Research	1	Basic principles observed and reported
	2	Technology and/or application concept formulated
Research and Development	3	Experimental proof of concept
	4	Validation of component(s) in a laboratory environment
	5	Validation of semi-integrated component(s) in a simulated environment
Pilot and Demonstration	6	System and/or process prototype demonstrated in a simulated environment
	7	Prototype system ready (form, fit and function) demonstrated in an appropriate operational environment
	8	Actual technology completed and qualified through tests and demonstrations
Early Adoption	9	Actual technology proven through successful deployment in an operational environment
Commercially Available		Technology development is complete

Table 1: TRLs suitable for broad research areas such as those at NSF. See footnote 36.

The earliest stage of research, TRL 1, is exploratory. Possible applications are often hypothesized at this stage, sometime generating a large amount of interest (e.g., high-temperature superconductors in the late 1980s) that is later tempered by further basic and applied research. The types of exploration are defined by the nature of the field and subfield. From TRL 1 work, which postulates and tests the fundamental principles of the field, will spring—at different times—pathways to different potential applications that are explored in TRL 2 and tested for basic feasibility in TRLs 3 and

[36]Government of Canada, "Technology Readiness Level (TRL) Assessment Tool," 2021, https://ised-isde.canada.ca/site/clean-growth-hub/en/technology-readiness-level-trl-assessment-tool. This is nearly identical to that used by the DOD, "Technology Readiness Levels in the Department of Defense (DoD)" in *Defense Acquisition Guidebook*, 2010, accessed December 21, 2023, https://api.army.mil/e2/c/downloads/404585.pdf.

4. As the emerging technologies move into validation stages at TRLs 4 and 5, practical issues such as the cost of the notional technology, the feasibility of manufacturing the technology reliably and at scale, and integration of the technology with other systems or environments, begin to impose substantial changes on the technical approach.

Generally, significant resources must be invested to move technologies from the R&D phase into the pilot and demonstration phase. Any organization that has assessed the outcomes of early-stage research will still need to make considerable investments to bring the work to a high TRL stage. This creates a natural barrier between the concept phase and the practical technology phase, where technologies begin to have demonstrable economic or national security significance. The key insight here is that while national security–sensitive concepts may seem apparent as early as TRLs 1 and 2, those concepts are subject to changes in approach and direction, and will likely require significant investments to mature before they transition to TRLs 5 and 6, where the actual national security significance can be demonstrated.

> **Finding:** The concept of Technology Readiness Level (TRL) is an essential component of the review to determine whether research is sensitive from a national security perspective.

4.5 Evaluating National Security Significance

In a national security evaluation, the designation of broad fields or sub-fields as sensitive or highly sensitive is problematic. Each field organizes itself in a different way, depending on history, funding, and culture. For example, quantum information science encompasses a range of work, such as materials science, device physics, and theoretical physics. Each sub-field has many different thrusts. Just choosing quantum sensors will still capture a spectrum of devices—gravitometers, plasmonic sensors, high-precision clocks, and so on—and each of those sub-sub-fields will have theory and multiple technical approaches at different TRLs, and with potentially entirely different national security impacts. Specific *projects* may need control, rather than their parent sub-fields.

> **Finding:** Differentiation between sensitive and non-sensitive research is most natural at the project level, not at the sub-field level. Projects in the same sub-field can have very different levels of risk.

A high TRL is not by itself a necessary or sufficient basis for deciding whether a research program merits additional mitigations or controls. The technology under

development must have national security significance, and the international state of R&D must be such that the applied protections would benefit U.S. national security. There might also be rare instances where fundamental research at low TRLs should be protected because of exceptional national security significance.

In deciding whether a technology has significant national security impact, NSF should consider the national security application goals, as well as any applications other than national security. If the development is aimed at an application outside national security, then NSF needs to consider whether the national security aspects are of such import that the need for protection overrides the social benefit of the non-national-security application. For example, a novel seismic monitoring system might improve the ability to characterize a country's explosive weapons testing, but NSF should ask whether the national security benefit of applying research controls to this research outweighs the benefit of developing capabilities that help mitigate earthquake hazards.

When reviewing these considerations, NSF should ask whether the technology is *sufficient and unique* for the national security use case in mind. It does not make sense to control emerging technologies, even at high TRLs, if they are not particularly suited to a national security use case. For example, precision clocks have national security applications, but precision is not by itself sufficient to constitute a national security concern; other factors such as low energy requirements and low physical volume must also be met before the clock becomes national security–sensitive.

Finally, before imposing any mitigations or controls, NSF needs to consider whether doing so would confer a meaningful advantage to the United States. In some domains of research, the United States might not be the leader, in which case international cooperation has the potential to elevate U.S. capabilities. In other cases, competition between the United States and a foreign country might be "neck and neck," in which case NSF should consider whether imposing the burden of security restrictions on U.S. researchers might slow the pace of U.S. innovation relative to foreign competitors. Mitigations and controls make the most sense when the United States has a definitive advantage and so can endure the burden of these protections without negatively impacting the country's relative position.

Overall, the discussion in this section sets the basis, further developed in Sections 5.1 and 6, of our response to Question 1 of the SOW (see Appendix A).

> **Finding:** Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that benefits outweigh the costs.

Recommendation: NSF should adopt a dynamic approach for identifying potentially sensitive research topics as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas. NSF's process of identifying sensitive research projects should:

- Differentiate research projects based on the sensitivity of their potential applications,
- Include the maturity of the development path (Technology Readiness Level—TRL) for potential applications in the assessment of risk, and
- Include an assessment of the direct and predictable national security impact of the applications of each research proposal, if successful.

This Page Intentionally Left Blank

5 RISK MITIGATION STRATEGIES FOR NSF

5.1 Mitigations and Controls

Figure 5 visualizes the range in mitigations and controls, depending on research sensitivity: no mitigation for most basic research; mitigations for *sensitive* research; controls for *highly sensitive* research—those areas for which the fundamental research exclusion (FRE) should no longer apply; Controlled Unclassified Information (CUI) controls as a subset of controls; and, finally, classification.

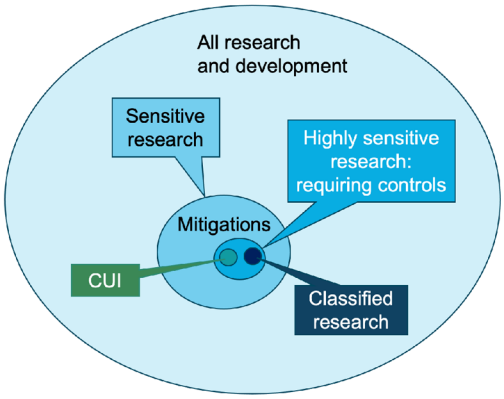

Figure 5: Categorization of NSF-funded research in terms of actions required to address sensitivity. *Sensitive* research generally requires mitigation measures—actions taken to protect sensitive research. *Highly sensitive* research generally requires controls; and for this category of research, the FRE does not apply. CUI and classified research are subcategories of controlled information. The areas of the research types depicted in the figure are not intended to be to scale. The fraction of NSF-funded academic research expected to be sensitive is small, and the fraction that is highly sensitive, even smaller.

A menu of possible mitigations and controls that provide a spectrum of protections, depending on the sensitivity of the research, follows. We recommend that NSF evaluate which of these mitigations or controls is appropriate on a project-by-project basis (see Section 6.1.1).

Mitigations Appropriate for Sensitive Research (FRE applies)

Possible mitigations include:

- Changes to the scope of a research grant,
- Training (or enhanced training) of the principal investigator (PI) on research security risk and protections,
- Enhanced training regarding publication of potentially sensitive results,
- Enhanced training on identifying individuals of concern who might be considered as possible participants or collaborators,
- Increased frequency or scope of reporting,
- Physical security standards for laboratories or computational facilities, and
- Cybersecurity standards for laboratory control systems or computing systems.

Controls for Highly Sensitive Research (FRE no longer applies)

Any of the above mitigations *plus* one or more of the following:

- Restrictions on participation for individuals of concern,
- Mandatory pre-approval for conferences or publication,
- Mandatory pre-approval before posting open-source data or software,
- CUI-like protections (see Appendix D and Section 5.2), and/or
- Funding contingent on accepting classification under Executive Order 13526.

Mitigations. In the case of *mitigations* for sensitive research, changes to the scope of a research grant are an easy way to limit potential accidental connections to sensitive topics. Training in research security awareness can be effective in helping reduce intellectual theft and ensuring that the benefits of research convey appropriately to U.S. entities. Such training will already be required per §10634 of the CHIPS and Science Act; but, in some cases, enhanced training focused on specific sensitivities

or extant compliance requirements may be valuable. Increased frequency or scope of reporting provides the opportunity for an NSF program officer to discuss aspects of sensitivity with the PI, as well as to get an update from the PI regarding evolution of the research toward possible applications. Finally, standards on physical security and cybersecurity are meant to prevent theft of valuable research results while not impeding the access of the researchers involved.

Controls. Any controls placed on research by NSF must be formally written as provisions in the grant or contract language accompanying the funding of the research. This is because controls and restrictions can place additional legal obligations on researchers that may require legal assistance and special training. In particular, acceptance of controls or restrictions voids the FRE, as explained in the definition of the FRE provided in Section 3 and discussed further in Section 5.3. Such controls should be reserved for highly sensitive research projects and include restrictions on participation of individuals and mandatory pre-approval of information dissemination. CUI is a type of control, but we judge its effectiveness to be limited (see Section 5.2 and Section D.5).

An alternative to imposition of controls by NSF is for NSF to simply not fund the research, or to refer the research to a more relevant funding agency—for example, the DOD. In some cases, this might be the most prudent action for NSF.

5.2 CUI as a Category of Research Control

NSF asked JASON, "What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?" While CUI controls may be appropriate for some research areas of particularly high sensitivity and risk, CUI is generally a rather blunt and ineffective tool for addressing the broad issue of U.S. research security. CUI should not be used as a one-size-fits-all approach to mitigating research risk.

As explained in Section 4.1, adequate protection of national security–sensitive information using CUI might require the definition of a new CUI-specified category defined by law, regulation, or government-wide policy. Regardless, all au-thorized holders of any type of CUI must:

- Establish controlled environments;
- Prevent unauthorized individuals from overhearing or observing CUI;

- Require direct control or physical barriers to CUI;
- Use only printers, copiers, and scanners that do not retain data;
- Delete electronic data in a method that makes the data irrecoverable; and
- Store, transmit, and process data only on information systems meeting the National Institute of Standards and Technology (NIST) SP 800-171 standard, which outlines 110 computer security provisions that must be satisfied.

The supporting apparatus for CUI-style access controls would impose significant cost on the conduct of research and reduce research funding efficiency.

In addition, we note that any access control is directly in conflict with the formal provisions of equal access to research that are in place at many universities. Such controls would disadvantage students involved with a controlled project by denying them the opportunity to engage in the free exchange of ideas, peer review, and practice at science communication. These activities are central to a student's education as scientist or engineer. As such, these controls compromise the educational mission of universities and NSF, and their necessity should be weighed against this cost.

Such controls would additionally impede creativity and innovation in the protected sectors. President Reagan's National Security Decision Directive (NSDD)-189 states that "an environment [with] the free exchange of ideas is a vital component" of academic research, and that such openness is therefore "an essential element in our physical and national security."[37] Slowing research in areas of national interest would impose a national security cost. Such negatives must be weighed against the benefit of preventing the controlled information from potentially leaking to foreign nations, realizing that if an adversarial peer country is determined to acquire the protected information, the controls are unlikely to stop them.

> **Finding:** Access controls create hindrances for education, the progress of science, and national security. These must be weighed against hypothesized gains in preventing information transfer, especially in the context of a sophisticated and determined adversary.

> **Finding:** CUI-required security controls could lead to increased cost of doing research, with a resulting loss in research efficiency.

[37] Office of the President of the United States, *National Policy on Transfer of Scientific, Technical and Engineering Information.* National Security Decision Directive 189. September 21, 1985, accessed December 21, 2023, https://catalog.archives.gov/id/6879779.

5.3 Consequences of Controls

NSF asked JASON, "What are some of the potential impacts on the research community should some NSF-funded research areas be designated as areas of concern?" We discuss these impacts here.

Loss of the Fundamental Research Exclusion (FRE). Given its importance, we discussed loss of the FRE earlier (see Section 3.1). This has a definite impact on those research areas designated as highly sensitive, putting researchers under legal obligation to prevent dissemination of the results of research to foreign nationals. This will be incompatible with the normal open discussion and exchange of ideas within universities. Some universities have stated their intent not to accept research funding with CUI or other controls because of this incompatibility.

Increased Cost of Research. Protecting controlled research may require financial resources, and thus increase the cost of doing research. For instance, holders of CUI-designated information will need to comply with numerous requirements including those for physical safeguarding of documents and equipment, as well as strict requirements concerning computer storage, transmission, processing, and cybersecurity (see Section D.5 for details). Facilities for proper handling of CUI-designated information will be a significant cost to the NSF grant or the performing institution. There is a risk that only a subset of research institutions can or will accommodate the increased security overhead required for controlled research projects.

Reducing the Number of U.S. Research Organizations Engaging in Fundamental Research Important to National Defense. It is highly desirable that the United States have strong fundamental research in areas that underpin technologies important to national defense. If a significant number of U.S. research organizations decide not to accept research funding that entails controls such as CUI, that will decrease the U.S. research base in those areas. As mentioned, some research institutions have already expressed their intent not to accept research funding with CUI controls. Other research institutions may not be able to participate in controlled research because of the increased overhead of implementing and maintaining facilities needed to handle protected equipment and information.

Shrinking the Talent Pipeline. Research with CUI and other export controls will limit participation of foreign nationals, regardless of their country of origin. NSF funding supports, both directly and indirectly, a significant fraction of advanced degree education in the United States, including the M.S. and PhD degrees of many foreign nationals studying in the United States. Many of these students remain in the United States after their degrees, contributing to the strength of the U.S. R&D effort,

with many becoming citizens. For its own sake, the United States should avoid the risk of creating an impression that it is not a welcoming place for foreign students.

Inhibiting Competitive Development of New Technologies. Open research is recognized as accelerating development of technology through competition, exchange of ideas via publication, and cross-fertilization of different research areas. Controls on dissemination of the results of research could slow the pace of innovation in areas of emerging technology where diversity of thought and active debate are most important. Because many technologies are dual-use, there also could be negative economic impacts. One other aspect is the potential limitation in the number of researchers who can participate in peer review of a controlled area of research. NSF depends on high-quality peer review for evaluation and selection of much of its research.

Possible Increased Bureaucratic Overhead at NSF. NSF is recognized as maintaining a relatively low in-house bureaucratic overhead. It does this through grants, contracts, and cooperative agreements to external organizations who then carry out the desired work. NSF follows this mode in the research security arena, for instance through its outsourcing of the development of training materials for research security (NSF Program Solicitation, NSF 22-276) and its recent solicitation for a Research Security and Integrity Information Center (NSF Program Solicitation, NSF 23-163). We commend NSF for these approaches, which allow NSF to address substantive issues in research security without building a large in-house organization.

The project-oriented identification and mitigation of research risk suggested for NSF in this report (see Section 6.1.1) must be carefully implemented so as not to produce an in-house bureaucracy centered around research security compliance. We note that NSF already has training programs for its staff in research security,[38] and it could build on these to implement the project-oriented research security approach recommended.

> **Finding:** Formal controls on research, such as a CUI designation, will have unintended consequences, including: increasing the cost of doing research, diverting resources better applied to expanding U.S. research efforts in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research.

[38] NSF, Office of the Chief of Research Security Strategy and Policy, "Research Security at the National Science Foundation—NSF Policies and Action," accessed December 21, 2023, https://new.nsf.gov/research-security#policies.

Recommendation: NSF should proceed with caution before adding access or dissemination controls to grants or contracts. In considering whether to apply formal controls to a sensitive research project, NSF should weigh the balance between the positive protective benefits and the unintended negative consequences of such controls. Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and national security interests.

This Page Intentionally Left Blank

6 A NATIONAL SCIENCE FOUNDATION APPROACH TO RESEARCH SECURITY

In this section, we put forth a framework for NSF to adjudicate research proposals that may enter the realm of sensitive or highly sensitive research. Our framework aims to integrate research security seamlessly with the overall proposal process. NSF has a strong history of effective proposal review, and we want that to continue, while also meeting the needs of research security. We start with the notion that a research project, rather than a research sub-field, presents the best basis for assessing risk to national security. Because NSF supports proposals that consist of research projects, reviewing a project offers a natural basis for this type of review and further action.

NSF asks its proposers to comment on the Broader Impacts[39] of their proposal, allowing them to provide information on the impact the proposed work may have beyond advancing the field. The Broader Impacts statement provides a natural place for NSF to solicit comments from the principal investigator (PI) on possible impacts on national security.[40]

The next section outlines an implementation approach that JASON recommends to NSF to ensure research security. Section 6.2, then, considers the role the universities and other research organizations can play in protecting national security without compromising their ability to carry out their mission. Section 6.3 describes proactive measures NSF, researchers, and universities can take to bolster U.S. national security, while still allowing open communication among researchers.

6.1 A Research Security Approach Tailored to NSF

Our investigations revealed the need for each agency to develop its own approach to protecting sensitive, unclassified information, which should reflect the agency's goals and missions (see Appendix C for a description of the approaches of other agencies). NSF has its own culture, procedures, and community. In particular:

[39] NSF, "Broader Impacts," https://new.nsf.gov/funding/learn/broader-impacts, accessed December 21, 2023.

[40] NSF, *Proposal & Award Policies & Procedures Guide (PAPPG), NSF 23-1* already lists "improved national security" in Chapter 2: Proposal Preparation Instructions, Part D Proposal Contents, 2023, accessed December 21, 2023, https://new.nsf.gov/policies/pappg/23-1/ch-2-proposal-preparation#2D2di). [21]

- A very large fraction of the research funded by NSF can be considered fundamental. Even within NSF's Directorate for Technology, Innovation, and Partnerships (TIP), a very small portion of research will ultimately be sensitive or highly sensitive.
- Unlike other U.S. R&D agencies, NSF does not manage laboratories that carry out research.[41] Rather, it funds research primarily through grants and contracts to outside organizations, mostly at universities or consortia of universities, with a broad range of capacities and missions.
- NSF funding is primarily awarded in response to proposals.
- NSF is extensively involved in international collaborations and is one of the principal U.S. agencies for funding of beneficial collaborations with foreign partners.
- Much of the NSF-funded research community is likely not aware of the full extent of research security concerns.

We considered the above points in formulating our specific recommendations.

6.1.1 A Proposal-Driven Approach

NSF responds primarily to proposals from university-based investigators, frequently with a single investigator who may have grants from several sources, or a group of investigators in a collaborative center. An NSF grant will typically run 3 to 5 years, and renewal remains competitive. While NSF program officers follow the work of those they fund, they usually do not exert supervisory control over their grantees' work.[42] They do receive an annual report of the PI's work on the award. The proposal cycle, including both the submission of a proposal and any subsequent review, provides the best, and perhaps only, opportunity to gain adequate insight into a project to determine whether that project entails sensitive research. Imposing substantial changes could require the creation of a new system within NSF, potentially adding to NSF's overhead. However, given the typical time and effort needed for a technology to move

[41] NSF funds 18 major scientific research facilities, such as the U.S. South Pole Station and the U.S. Academic Research Fleet, where NSF retains discretion as to the scope of research carried out; however, for the most part, NSF does not direct research at these facilities. Research security for these large NSF facilities is a separate topic, not addressed in this report.

[42] The NSF *PAPPG* does not require any annual reporting of the progress of funded work, although it does encourage regular contact between the program officer and awardee. See Chapter 7: Award Administration, A. Monitoring Project Performance, in *PAPPG, NSF 23-1*, 2023, accessed December 21, 2023, https://new.nsf.gov/policies/pappg/23-1/ch-7-award-administration#7A1. [21]

from application concept to maturity, we assess that reviewing sponsored work on a 3- to 5-year basis provides a good starting point.

> **Finding:** The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects—i.e., those projects for which the release of information about research execution or outcomes could have a significant, direct, and predictable impact on national security.
>
> **Recommendation:** The identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. We recommend that the principal investigator (PI) and the NSF program officer, with guidance from the NSF Division Office, determine if a proposal constitutes a sensitive project. NSF may wish to implement a pilot program within some division of NSF to gain experience with the process. NSF should consult with other federal research funding agencies such as the Department of Energy (DOE), the National Institutes of Health (NIH), and the Department of Defense (DOD) to help identify sensitive research.

JASON recognizes that NSF does not currently have the in-house national security expertise to implement the preceding recommendation across all its relevant programs. Building up the requisite knowledge and expertise will be a long-term endeavor over several years. However, JASON believes that to address research security effectively, NSF *must* work toward developing an in-house culture of research security awareness and developing sufficient in-house expertise to be able to identify sensitive research. NSF could also consult with external experts to aid in its evaluation. Because of its unique portfolio of funded research, NSF is in the best position to assess on a project-by-project basis which projects might include sensitive or highly sensitive research.

> **Finding:** In order to effectively evaluate proposed research for potential sensitivity, NSF will need to develop in-house national security expertise. NSF staff with appropriate expertise would serve as consultants to support the review process.

JASON finds that the present NSF proposal-review process would work well for the purpose of identification of sensitive projects, although some modifications will be needed. Below, we describe the elements needed to add a process for identifying and adjudicating support for sensitive or highly sensitive projects without hampering the overall proposal process.

Each NSF division should develop standard guidelines about potential national security implications in its research areas to facilitate an earnest self-assessment by the

PIs. NSF should provide the tools and guidance to enable researchers to perform the assessment with minimal time burden to the research community.

We emphasize that the proposal-driven approach we recommend is quite different from the list-based approach that JASON was asked to comment on in the Statement of Work (SOW) from NSF (see Appendix A). Relying on lists of broad research areas of possible concern will be inadequate for reliably identifying specific research projects that are sensitive or highly sensitive. To be effective, the lists of sensitive research areas would need to be so granular and detailed as to be unwieldy. Such an approach would thus require a large effort to develop, approve, maintain, and update these lists across the agency. We therefore recommend a *process* for NSF to identify sensitive research, rather than a list-based approach. We describe this process next.

6.1.2 Initial PI Evaluation

The suggested process starts with a self-evaluation by the project's PI at the time the proposal is submitted. Typically, the PI understands the research better than anyone else, and NSF should take advantage of this knowledge, while also recognizing that self-evaluation is not by itself sufficient.

As part of preparing materials for submission, the PI would be asked to list the expected outcomes or applications of the research. We suggest NSF ask the PI to state whether, in their view, the proposed project has potential national security impact based on guidelines NSF would develop. If the PI marks the project as potentially sensitive, the PI should be asked to provide the following information:

- The intended use (if any) of the results of the project;
- The Technology Readiness Level (TRL) of the work initially, and that expected at the end of the project; and
- Whether the technology has features that create national security impact beyond that of technology already discussed in the open literature.

PIs will need guidance on how to assess their proposals. Only a small percent of projects will lie close to sensitive or highly sensitive research. In the large majority of non-sensitive cases, the PIs need only provide a sentence or two about why their project does not have national security sensitivity based on the NSF-developed guidelines.

> **Recommendation:** JASON recommends NSF develop language for the *Proposal & Award Policies & Procedures Guide (PAPPG)* to help PIs assess their proposed projects for possible impact on national security, including providing guidelines on what may, or may not, constitute research with potential national security impact.

6.1.3 NSF Review

Upon receiving a proposal, regardless of how it is marked by the PI, the NSF program officer (or designee) should review the researcher's evaluation of potential sensitivity and formulate their own assessment. At this step, the program officer must decide whether to request the information above, if it has not already been provided in the PI's self-assessment. If the proposed research is not deemed sensitive, the program officer will move it through the review process as normal. If the proposed research is considered to constitute a potentially sensitive or highly sensitive project, the NSF division, NSF program, and perhaps the PI will have to work together to have the proposal appropriately reviewed. JASON recommends that NSF appoint a group of NSF staff with national security expertise to support such reviews in concert with the program officer, the division director, and others in NSF. This in-house group could also serve as consultants later in the process. The final decision about supporting any proposal must lie with the chain of command within the division—as it does now. Those providing national security expertise remain as advisors, not as reviewers.

> **Finding:** Initial assessment by the principal investigator (PI), with review by the NSF program office (and perhaps the NSF parent division), provides the best screening for potentially sensitivite or highly sensitive proposals—i.e., those that may need mitigations or controls.

The primary criterion for risk should be whether the research will have significant, direct, and predictable impact on national security.

> **Recommendation:** Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the sponsored projects office of the institution accepting responsibility for execution of the research. Specific mitigation steps should be proportionate to the assessed risk, relative to the associated costs.

6.1.4 Protecting Sensitive Projects

If a project involving sensitive or highly sensitive research is selected for potential funding, NSF will have to determine a mitigation plan with the research institution and the PI. Owing to the broad spectrum of work supported by NSF, specific mitigations or controls for sensitive or highly sensitive projects must be determined on a case-by-case basis. NSF's in-house national security experts can help guide the selection of appropriate mitigations or controls. Ultimately, though, all stakeholders—the PI, NSF program officer, and the institution's sponsored program office—must agree upon an appropriate way forward with the project. Any controls placed on the research by NSF must be formally written as provisions in the grant or contract language accompanying the research funding. The specific mitigations or controls applied should be based on an evaluation of relative benefits and drawbacks of applying such protections. Possible mitigations and controls, and their consequences, are discussed in Section 5.1. During this review, considerations should include:

- How the intended, or realistically foreseeable, uses of the technology might impact U.S. national security.
- The relative stage of advancement of the United States versus other countries in the research area.
- The impact of restrictions on the ability of some researchers to work on the project.
- The impact controls on communication of results of the research may have on the PI's ability to successfully carry out the research, and on the community at large.
- Additional costs, financial and otherwise, of the proposed mitigations or controls.

NSF might consider the formation of divisional boards for the purpose of assessing the risk associated with research activities proposed by PIs funded by NSF, perhaps in affiliation with other government agencies. These divisional boards would work cooperatively with university administration and proposers to determine, based on technical assessments, whether proposed research poses risk so as to be subject to restrictions currently being codified to enforce research security.

6.2 The Role of Research Institutions Such as Universities

NSF funds research institutions, such as universities, to carry out much of the research it supports. Consequently, research institutions and their PIs will be responsible for the actual implementation of research security measures. Their role will be critical. Research institutions have several responsibilities in the research security process, including:

- Working with NSF and other agencies to provide input on proposed research security guidelines and requirements.
- Ensuring that researchers at their institutions working in areas of sensitive or highly sensitive research are informed and trained in research security awareness.
- Understanding and signing off on research security guidelines and requirements in federal grants and contracts.
- Ensuring compliance with research security actions.

Finding: Research institutions and NSF have key roles to play in the process of risk identification and management. Dialogue between NSF and research institutions such as universities is critical.

Recommendation: The NSF Office of Research Security should initiate meetings and forums with universities to discuss its plans for research security and to solicit input and feedback on its procedures once they begin to be implemented. This can begin now with respect to research security training modules being developed by NSF. If NSF initiates a pilot program for the identification of sensitive or highly sensitive research and its mitigation and control, feedback from universities will be vital for tuning the program for wider implementation across the entire scope of NSF-funded research.

6.3 Proactive Steps

So far, our discussion has focused primarily on *protective* steps to enhance research security. Protective steps are aimed at lowering the risk that critical technology will be appropriated and exploited by foreign countries. However, protective steps are insufficient to address the issue of maintaining U.S. leadership in critical technology

areas. We therefore discuss several *proactive* steps to enhance the capabilities of the U.S. research enterprise in the interests of national security.

Building a Culture of Research Security Awareness.
Research security will be enhanced if individuals in the research community are aware both of the importance of research security and of the risks to that security that may exist in the research environment. Most individuals in the U.S. academic research community are relatively unaware of both the importance and the full extent of research security risks. Consequently, building a culture of awareness of research security in the United States will be a long-term, non-trivial task. However, it is JASON's view that researchers receiving federal funding for their work have a responsibility to protect the interests of the United States; therefore, it is incumbent on universities and NSF to foster an awareness of security issues related to research.

> **Finding:** Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level, and such steps are mandated under the CHIPS and Science Act.

> **Recommendation:** NSF should foster a culture of research security awareness by providing substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions about the efficacy of research risk mitigation and control efforts.

A researcher working in a potentially sensitive area of research will be faced with numerous questions: Should I hesitate to publish these research findings? Should I work with this other individual on this sensitive research? Whom should I consult if I am not sure? These are not trivial questions, and intentional, proactive steps are needed to encourage academic practitioners to adopt behaviors that serve, collectively and over time, to reduce the probability and severity of adverse outcomes.

There is extensive literature on how to shape *safety* culture within organizations (see Uttal, 1983 [22]; and Reason, 1990, 1997, and 1998 [23, 24, 25]). While building a research security culture will be different from shaping a safety culture, there are many common considerations. The published work on security culture is less academic and more focused on best practices. Recurring themes include: risk awareness; simple, uniform, and transparent policies; security assessment; positive incentives; and communication of security priorities by leadership.

Translated into actionable steps, these themes could include:

- Designing security procedures in such a way that researchers understand what is being protected and how to implement the procedures effectively.
- Providing researchers with substantive information and examples concerning real risks.
- Providing resources for researchers to ask for research security guidance.
- Providing researchers a confidential mechanism to report concerns ("if you see something, say something"). Researchers will need to understand that their concerns will not result in bias against, or profiling of, colleagues.

We note that the CHIPS and Science Act[43] mandates that NSF establish a research security and integrity information sharing analysis organization (RSI-ISAO). The responsibilities specified for this organization in the CHIPS and Science Act include:

- "Serve as a clearinghouse for information to help enable the members and other entities in the research community to understand the context of their research and identify improper or illegal efforts by foreign entities to obtain research results, know how, materials, and intellectual property"
- "Develop a set of standard risk assessment frameworks and best practices, relevant to the research community, to assess research security risks in different contexts"
- "Share information concerning security threats and lessons learned from protection and response efforts through forums and other forms of communication"
- "Provide training and support, including through webinars, for relevant faculty and staff employed by institutions of higher education on topics relevant to research security risks and response"

Finding: Properly implemented, a research security and integrity information sharing analysis organization (RSI-ISAO) of the type described in the CHIPS and Science Act would be a proactive step toward ensuring the security of the U.S. research enterprise and would provide tools and support for the development of a culture of awareness for research security.

[43]CHIPS and Science Act, Section 10338(b).

We further note that the CHIPS and Science Act[44] also mandates a security training requirement for federal research award personnel. Security training modules[45] can be one component of a toolkit for addressing research security. However, care must be taken in the implementation of security training modules. Requirements and resources should be focused on areas of greatest risk.

We suggest that full security training should be required for those individuals working in areas of higher risk for research security, with reduced levels of training for those in low-risk areas. Requiring all researchers in all fields to take the full suite of available security training modules would be, in our opinion, an inefficient use of U.S. federal funding and university institutional resources. It may also be counterproductive, in that it could engender negative attitudes toward research security efforts.

> **Finding:** Training is an important component of an overall program to enhance research security. However, training will be most effective, in terms of impact and human resources, if required primarily in research areas where the security risk is highest.

Capitalizing on Relationships with International Allies.
Science is international in character and promotes efficiency and effective validation of results—similar to the rationale for openness and transparency of U.S. research applied more generally to the world at large. The United States benefits from other countries replicating our results, just as we benefit from seeing and learning from their new results. These arguments have become stronger over recent decades, as more nations around the world participate at the state-of-the-art level in the research enterprise (see, e.g., American Academy of Arts and Sciences–AmAcad–(2020)[26] and (2022)[27]).

U.S. allies in the European Union (EU), Asia-Pacific, North America, and elsewhere share many of the concerns about academic research security addressed in this report. We see at least two opportunities for leveraging international cooperation with like-minded colleagues in this domain.

- Discussions between NSF and counterpart organizations that fund basic scientific research in the EU and elsewhere could involve sharing best practices for suitably protecting sensitive and highly sensitive information while still enhancing the benefits that science brings to our nations' common security and prosperity. There is an opportunity to learn from allies' perspectives and to

[44]CHIPS and Science Act, Section 10634.
[45]CHIPS and Science Act, Section 10634(c).

identify how best to sustain existing cooperative scientific programs with those nations. One example is the report of the European Commission on foreign interference in research and innovation.[46] Another is the Trusted Research Program of the United Kingdom (UK) National Protective Security Authority,[47] which has many themes in common with current NSF research security initiatives. International cross-agency cooperation on the difficult topic of protecting sensitive and highly sensitive information could enhance existing scientific collaborations and strengthen the community's ability to counter threats from more secretive nations' research programs.

- Scientific societies already play a role in setting international standards of professional conduct and ethics. They could help inform researchers about how to establish and maintain balanced collaborations and other working relationships in a manner that is mutually beneficial (i.e., avoiding one nation systematically taking advantage of another.) While not a task for NSF itself, U.S. researchers should engage with international scientific societies to promote best practices of openess and fairness internationally.

Finding: There is an opportunity for NSF to work with counterpart funding agencies in nations supporting open and transparent scientific research so as to sustain the benefits to society of basic scientific research while minimizing the damage caused by necessary controls of sensitive information.

Recommendation: NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

Addressing Shortages in the U.S. Science, Technology, Engineering, and Mathematics (STEM) Workforce.
A significant consideration is that the United States has long benefited from foreign students obtaining degrees and starting their careers in U.S. schools, laboratories, and companies, with more than 100,000 U.S. higher-education degrees now being given to foreign students each year (JASON, 2019 [17]; Congressional Research Service (CRS), 2019 [29]). Historically, 70 percent of foreign (including 80–90 percent of Chinese) doctoral recipients choose to stay in the United States after completion of their degree.

[46]Directorate-General for Research and Innovation (European Commission), *Tackling R&I Foreign Interference — Staff Working Document*, Publications Office of the European Union, 2022, accessed December 21, 2023, https://data.europa.eu/doi/10.2777/513746. [28]

[47]U.K. National Protective Security Authority, "Trusted Research," accessed December 21, 2023, https://www.npsa.gov.uk/trusted-research.

The need for STEM students is currently so intense that the United States faces a shortfall of 5,000 students per year, in terms of U.S. persons gaining the necessary education. Foreign students, mainly from China and India (see, e.g., CRS, 2019 [29]; AmAcad (2022) [27]), make up that shortfall and help us maintain the influx of early-career researchers needed to sustain our STEM-based workforce of about 36 million[48] and GDP growth of 3 percent, driven in part by R&D innovations (see also the discussion in Section 2.4).

Through foreign students and collaborators, U.S. researchers develop a detailed understanding of the level of technical expertise present around the world, to the point of being able to identify the best educational or research programs abroad. Finally, foreign graduates from U.S. programs who return to their home country carry with them an understanding of our values and procedures, which is of long-term benefit to the United States. The same can be said of foreign research collaborations.

A challenge is how to improve research security while simultaneously ensuring that foreign students continue to see the United States as an attractive, welcoming, and open place to engage in research. NSF has an important role to play, through careful communication of the goals of its research security programs, together with its strong continuing support for research programs open to foreign students.

Increasing Investment in Technical Areas of Importance to National Security.
As discussed in Section 2.4, strategic R&D investments and the development of the U.S. STEM workforce need to be priorities for the United States. With regard to NSF, the recent establishment of the TIP Directorate, part of the CHIPS and Science Act directives, represents an investment toward development of strategic technologies.

With regard to the STEM workforce, increasing the number of degree-earning U.S. students in key technical areas should be a priority, particularly if the number of foreign students doing research in the United States declines—for example, because of increased international competition for such students. NSF could consider training grants for U.S. students in research and technology areas that are most relevant for national security.

NSF project funding is primarily awarded through a merit-based selection process that considers novelty, impact, and significance. NSF also funds people, by virtue of the NSF Graduate Research Fellowship Program (GRFP), without constraints on the type of work that the recipients perform during their fellowship tenure. Recipients

[48] National Science Board (NSB), *The State of U.S. Science and Engineering,* Figure 8, NSB-2022-1, https://ncses.nsf.gov/pubs/nsb20221/

of NSF GRFP funding must be U.S. citizens. In contrast, graduate students and post-doctoral researchers of any nationality are eligible for support in NSF-sponsored projects. These two funding mechanisms have served NSF well and are consistent with NSF policies on open science and open data, as well as the open science policies of universities.

As a technology evolves from fundamental research toward applications, and specifically toward applications that may be readily transitioned and exploited for national security uses, it would be beneficial to train more domestic students to enter the U.S. workforce in associated fields. We suggest that NSF consider a new funding program in targeted areas of national security significance that would help achieve this goal. In those areas, NSF could offer both training grants and post-doctoral fellowships as a tool to strengthen research security and provide enhanced training for a domestic science and engineering workforce. Annual meetings could be convened for the cohort of supported graduate students and post-doctoral fellows to build a community. Such a funding mechanism might be especially attractive for implementation as part of the newly established NSF TIP program. While other agencies, such as the NIH and the DOD, have similar funding programs, NSF may be able to engage a different segment of the future STEM workforce.

This Page Intentionally Left Blank

7 SUMMARY

In this report, we have considered the question of how NSF should address the issue of research security in its funded research programs. This report recommends specific steps that NSF can take to enhance awareness of research security, both within NSF and in the research community. It also suggests mechanisms for NSF to address research projects that are identified as sensitive because of their possible impact on national security. The processes we describe are compatible with the existing NSF structure and its emphasis on funding of research proposals from individual researchers and research organizations. The processes are flexible and adaptable so that they can respond to changing conditions and thinking about research security. While our recommendations focus on academic research security, many are relevant to NSF-funded R&D at organizations other than institutions of higher learning.

We provide the complete findings and recommendations of this study in the order they are discussed. The findings and recommendations are labeled with the relevant section number of the report—e.g., the label "F4-2" indicates the second finding in Section 4. Bold text indicates a key finding or recommendation also contained in the Executive Summary of this report.

7.1 Findings

F1-1 Openness and transparency in fundamental research promote scientific discovery, which improves national security.

F2-1 International collaborations with those who share the ideals of openness and transparency benefit all participants. However, recent efforts of the People's Republic of China (PRC) to preferentially direct fundamental research toward military needs, and its decision to restrict the flow of information out of the country, may severely limit the benefits of collaborations with research organizations within the PRC.

F4-1 The existing categories of Controlled Unclassified Information (CUI) do not provide useful guidance for identifying sensitive research that might be funded by NSF. The CUI guidelines themselves are silent as to what kinds of information need protecting.

F4-2 The Department of Energy (DOE) approach involves identifying specific critical areas of emerging technologies and utilizing subject matter experts in evaluating the sensitivity of the research. Regular updating and implementation of this scheme is labor intensive.

F4-3 At early stages of research, the potential applications' outcomes are notional. Most commonly, highly ambitious potential applications postulated for early-stage research are later replaced with different potential applications, addressing a range of societal, commercial, and national security needs as the research area progresses in technical maturity.

F4-4 The concept of Technology Readiness Level (TRL) is an essential component of the review to determine whether research is sensitive from a national security perspective.

F4-5 Differentiation between sensitive and non-sensitive research is most natural at the project level, not at the sub-field level. Projects in the same sub-field can have very different levels of risk.

F4-6 Risk mitigation must consider the spectrum of risk and be adaptable to changing trends in research. Resources should be concentrated on areas of maximum risk to ensure that benefits outweigh the costs.

F5-1 Access controls create hindrances for education, the progress of science, and national security. These must be weighed against hypothesized gains in preventing information transfer, especially in the context of a sophisticated and determined adversary.

F5-2 CUI-required security controls could lead to increased cost of doing research, with a resulting loss in research efficiency.

F5-3 Formal controls on research, such as a CUI designation, will have unintended consequences, including: increasing the cost of doing research, diverting resources better applied to expanding U.S. research efforts in critical fields, inhibiting rigorous and competitive development of new technologies, and discouraging some individuals and research organizations from engaging in U.S. research.

F6-1 The NSF proposal and reporting cycle provides the most natural means for identifying sensitive projects—i.e., those projects for which the release of information about research execution or outcomes could have a significant, direct, and predictable impact on national security.

F6-2 In order to effectively evaluate proposed research for potential sensitivity, NSF will need to develop in-house national security expertise. NSF staff with appropriate expertise would serve as consultants to support the review process.

F6-3 Initial assessment by the principal investigator (PI), with review by the NSF program office (and perhaps the NSF parent division), provides the best screening for potentially sensitivite or highly sensitive proposals—i.e., those that may need mitigations or controls.

F6-4 Research institutions and NSF have key roles to play in the process of risk identification and management. Dialogue between NSF and research institutions such as universities is critical.

F6-5 Awareness of research security issues among university researchers is lower than warranted at present, but approaches are available to raise the awareness level, and such steps are mandated under the CHIPS and Science Act.

F6-6 Properly implemented, a research security and integrity information sharing analysis organization (RSI-ISAO) of the type described in the CHIPS and Science Act would be a proactive step toward ensuring the security of the U.S. research enterprise and would provide tools and support for the development of a culture of awareness for research security.

F6-7 Training is an important component of an overall program to enhance research security. However, training will be most effective, in terms of impact and human resources, if required primarily in research areas where the security risk is highest.

F6-8 There is an opportunity for NSF to work with counterpart funding agencies in nations supporting open and transparent scientific research so as to sustain the benefits to society of basic scientific research while minimizing the damage caused by necessary controls of sensitive information.

7.2 Recommendations

R4-1 NSF should adopt a dynamic approach for identifying potentially sensitive research topics as they arise, instead of attempting to maintain a comprehensive list of sensitive research areas. NSF's process of identifying sensitive research projects should:

- Differentiate research projects based on the sensitivity of their potential applications,
- Include the maturity of the development path (Technology Readiness Level—TRL) for potential applications in the assessment of risk, and
- Include an assessment of the direct and predictable national security impact of the applications of each research proposal, if successful.

R5-1 NSF should proceed with caution before adding access or dissemination controls to grants or contracts. In considering whether to apply formal controls to a sensitive research project, NSF should weigh the balance between the positive protective benefits and the unintended negative consequences of such controls.

Controls can protect U.S. national security by preventing malign use of research results, but they can also hinder the beneficial free flow of research results in a way that negatively impacts broader U.S. economic and national security interests.

R6-1 The identification of sensitive projects proposed to NSF occurs most naturally before peer or panel review. We recommend that the principal investigator (PI) and the NSF program officer, with guidance from the NSF Division Office, determine if a proposal constitutes a sensitive project. NSF may wish to implement a pilot program within some division of NSF to gain experience with the process. NSF should consult with other federal research funding agencies such as the Department of Energy (DOE), the National Institutes of Health (NIH), and the Department of Defense (DOD) to help identify sensitive research.

R6-2 JASON recommends NSF develop language for the *Proposal & Award Policies & Procedures Guide (PAPPG)* to help PIs assess their proposed projects for possible impact on national security, including providing guidelines on what may, or may not, constitute research with potential national security impact.

R6-3 Specific mitigation strategies for sensitive research projects should be negotiated and agreed upon by the principal investigator (PI), NSF, and the sponsored projects office of the institution accepting responsibility for execution of the research. Specific mitigation steps should be proportionate to the assessed risk, relative to the associated costs.

R6-4 The NSF Office of Research Security should initiate meetings and forums with universities to discuss its plans for research security and to solicit input and feedback on its procedures once they begin to be implemented. This can begin now with respect to research security training modules being developed by NSF. If NSF initiates a pilot program for the identification of sensitive or highly sensitive research and its mitigation and control, feedback from universities will be vital for tuning the program for wider implementation across the entire scope of NSF-funded research.

R6-5 NSF should foster a culture of research security awareness by providing substantive information to researchers about real risks, making resources available for researchers to voluntarily seek guidance, and continuously engaging with researchers and their institutions about the efficacy of research risk mitigation and control efforts.

R6-6 NSF should engage in dialogue with international partners who have like-minded approaches to research security and integrity, and who are facing similar research security problems.

References

[1] Daniels, Mario and John Krige. *Knowledge Regulation and National Security in Postwar America*. Chicago: University of Chicago Press, 2022.

[2] National Academies of Sciences, Engineering, and Medicine, Committee on Science, Engineering, and Public Policy. *Scientific Communication and National Security*. Washington, DC: The National Academies Press, 1982. https://doi.org/10.17226/253.

[3] National Science and Technology Council, Subcommittee on Research Security, Joint Committee on the Research Environment. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) On National Security Strategy for United States Government-Supported Research and Development*, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf.

[4] National Science and Technology Council, Office of Science and Technology Policy, Subcommittee on Research Security. *Draft Research Security Programs Standard Requirement*, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf.

[5] Hannas, William C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*. New York: Routledge, 2013.

[6] The White House. "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy", October 12, 2022. https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/10/13/remarks-by-national-security-advisor-jake-sullivan-on-the-biden-harris-administrations-national-security-strategy/.

[7] The White House. "President Biden Signs Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern." Press release, August 09, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/08/09/president-biden-signs-executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/.

[8] National Science Foundation, National Science Board. *Science and Engineering Indicators, Research and Development: U.S. Trends and International Comparisons, NSB 2022-5*, 2022. https://ncses.nsf.gov/pubs/nsb20225.

[9] Fedasiuk, Ryan, Alan Omar Loera Martinez, and Anna Puglisi. "A Competitive Era for China's Universities: How Increased Funding is Paving the Way". *Center for Security and Emerging Technology (CSET)*, March 2022. https://cset.georgetown.edu/wp-content/uploads/CSET-A-Competitive-Era-for-Chinas-Universities.pdf.

[10] National Science Foundation, National Science Board. *Science and Engineering Indicators, Publications Output: U.S. Trends and International Comparisons, NSB-2021-4*, 2021. https://ncses.nsf.gov/pubs/nsb20214/international-collaboration-and-citations.

[11] Remco, Zwetsloot, Jack Corrigan, Emily S. Weinstein, Dahlia Peterson, Diana Gehlhaus, and Ryan Fedasiuk. "China is Fast Outpacing U.S. STEM PhD Growth". *Center for Security and Emerging Technology (CSET)*, 2021. https://doi.org/10.51593/20210018.

[12] National Science Foundation, National Science Board. *Science and Engineering Indicators 2022, The State of U.S. Science and Engineering 2022, NSB-2022-1.* https://ncses.nsf.gov/pubs/nsb20221/conclusion.

[13] PRC Ministry of Science and Technology. "The '13th Five-Year' Special Plan for S&T Military-Civil Fusion Development". Center for Security and Emerging Technology (CSET), 2020. https://cset.georgetown.edu/publication/the-13th-five-year-special-plan-for-st-military-civil-fusion-development/.

[14] Jash, Amrita. "China's Military-Civil Fusion Strategy: Building a Strong Nation with a Strong Military". *Claws Journal*, 13(2):42–62, 2020. https://www.neliti.com/publications/330719/chinas-military-civil-fusion-strategy-building-a-strong-nation-with-a-strong-mil.

[15] Bitzinger, Richard A. "China's Shift from Civil-Military Integration to Military-Civil Fusion". *Asia Policy*, 16(1), 2021.

[16] People's Republic of China. *Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035*, 2021. https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

[17] Long, Gordon. *Fundamental Research Security: JASON Report* JSR-19–21. McLean, VA: MITRE Corporation, 2019. https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[18] Foster, Richard N. "Working the S-Curve: Assessing Technological Threats". *Research Management*, 29(4):17–20, 1986.

[19] Ergin, Tolga, Nicolas Stenger, Patrice Brenner, John B. Pendry, and Martin Wegener. "Three-Dimensional Invisibility Cloak at Optical Wavelengths". *Science*, 328(5976):337–339, 2010. https://www.science.org/doi/10.1126/science.1186351.

[20] Jacobs, Josh. "'Invisibility Cloak' Metamaterials Make Their Way Into Products". *Financial Times*, 2018. https://www.ft.com/content/c6864c76-de7d-11e7-a0d4-0944c5f49e46.

[21] National Science Foundation. *Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 23-1)*, 2023. https://new.nsf.gov/policies/pappg.

[22] Uttal, Bro. "The Corporate Culture Vultures". *Fortune*, 108(8):66–72, 1983.

[23] Reason, James. *Human Error*. Cambridge: Cambridge University Press, 1990.

[24] Reason, James. *Managing the Risks of Organizational Accidents*. London: Routledge, 1997.

[25] Reason, James. "Achieving a Safe Culture: Theory and Practice". *Work & Stress*, 12(3):293–306, 1998.

[26] Challenges for International Science Partnerships (CISP). *America and the International Future of Science*, 2020. American Academy of Arts and Sciences, Cambridge, MA, https://www.amacad.org/publication/international-science.

[27] Challenges for International Science Partnerships (CISP). *Global Connections: Emerging Science Partners*, 2022. American Academy of Arts and Sciences, Cambridge, MA, https://www.amacad.org/sites/default/files/publication/downloads/2022-CISP_Global-Connections-Emerging-Science-Partners.pdf.

[28] Directorate-General for Research and Innovation (European Commission). *Tackling R&I Foreign Interference – Staff Working Document*, 2022. https://data.europa.eu/doi/10.2777/513746.

[29] Granovskiy, Boris and Jill Wilson. *Foreign STEM Students in the United States. CRS Report IF11347*. Congressional Research Service, 2019. https://crsreports.congress.gov/product/pdf/IF/IF11347.

[30] Ison, Jeremy. "Update for COGR on Research, Technology and Economic Security", 2023. U.S. Department of Energy, Office of Science. https://www.cogr.edu/sites/default/files/Multi-Agency%20Research%20Security%20Panel_0.pdf.

This Page Intentionally Left Blank

Appendix A STATEMENT OF WORK

Study Background:

In the 2019 JASON report on "Fundamental Research Security," JASON assessed whether any type of fundamental research needed to have additional controls imposed. The JASON report assessed the concept of "Controlled Unclassified Information" and confusion attendant to that concept and recommended that control of research should be as stated in National Security Decision Directive 189 (NSDD-189). Namely, NSDD-189 stated that the method for control of research essential to national security should be the formal classification system, and that the products of fundamental research should be unrestricted.

In the three years since the 2019 JASON report was completed, there has been much discussion in the U.S. government and elsewhere about whether particular research or technology areas need further protection or safeguards. Various federal agencies have attempted to define critical technologies and to develop lists of technology that may need further protection, but the U.S. government has found it challenging to articulate the need for protection or safeguards in a way that is useful to the research community and that does not shut off the open flow of information that enables the research enterprise to succeed.

CHIPS-and-Science Act

Section 10339 of the CHIPS-and-Science Act passed in 2022 imposes a new requirement on NSF, specifically to "identify research areas ... that may involve access to controlled unclassified or classified information" and "exercise due diligence in granting access ... to individuals working on such research who are employees of the Foundation or covered individuals on research and development awards funded by the Foundation." This may be particularly, though not exclusively, relevant to the new Directorate for Technology, Innovation, and Partnerships that was initiated by NSF in 2022.

Congressional FY23 Appropriations Language

Congress clarified its guidance to the NSF in its FY23 Appropriations bill:

> "**Open Source Research Risks**.—The Committee is concerned that certain open source research capabilities at NSF could be used by adversaries against U.S. allies or U.S. interests. The Committee therefore directs the

> NSF to collaborate with the Secretary of Defense and the Director of National Intelligence to compile and maintain a list of all NSF-funded open source research capabilities that are known or suspected to have an impact on foreign military operations. Such list shall be reviewed and updated at least annually by the NSF in collaboration with the Secretary of Defense and the Director of National Intelligence, and subsequently shall be reported to the Committee."

Objectives:

NSF seeks advice on how to identify the research areas referenced in Section 10339 of the CHIPS and Science Act of 2022, and how to decide when research crosses into the realm that may need control. Such controls may also impact both the quality and quantity of research, as well as the translation of research results into benefits for the nation. Given the broad scope of research that could be affected, JASON should combine general considerations with a detailed assessment of one or more particular research/technology areas, such as quantum information science. Such a detailed assessment could lead to development of a set of questions or evaluation criteria that NSF might use in fulfilling the Section 10339 requirements and Congressional guidance for maintaining a list of NSF-funded research areas of concern.

Specific questions to be addressed in the JASON study:

1. What are the general principles that NSF might use in developing lists of research/technology areas of concern?
2. What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?
3. What processes might NSF establish for annually reviewing its list of research/technology areas of concern?
4. Using one or more specific research/technology areas, as examples, what detailed evaluation criteria might NSF use for identifying research/technology areas of concern?
5. What are some of the potential impacts on the research community should some NSF- funded research areas be designated as areas of concern?
6. What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?

Appendix B JSR-19-2I EXECUTIVE SUMMARY

A previous JASON Report JSR-19-2I,[49] discussed the issue of research security for fundamental research. We provide the Executive Summary of that report for reference.

[49]Gordon Long, "JSR-19-2I Fundamental Research Security," MITRE Corporation (2019), accessed December 18, 2023, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf. [17]

EXECUTIVE SUMMARY: JASON REPORT JSR-19-2I, *Fundamental Research Security*

The National Science Foundation (NSF) celebrates its 70th anniversary this year (2019). Over seven decades it has transformed U.S. fundamental research and enabled a world-leading scientific enterprise built upon open intellectual exchange, collaboration, and sharing. Several incidents in recent years have led to concern that the openness of our academic fundamental research ecosystem is being taken advantage of by other countries. This sense of unfair competition is entwined with concerns about U.S. economic and national security in a rapidly changing world. The NSF wishes to assess these concerns and respond to them where appropriate, while also adhering to core values of excellence, openness, and fairness.

NSF has charged JASON to produce an unclassified report that can be widely disseminated and discussed in the academic community, providing technical or other data about specific security concerns in a classified appendix.

JASON was asked:

1. What is the value and what are the risks of openness generally associated with fundamental research?

2. How should the principles of scientific openness be affirmed or modified?

3. Are there areas of fundamental research that should be more controlled rather than openly available? What are those areas?

4. What controls, if any, could be placed on particular types of information, and how can this be managed in a way that maintains the maximum benefit of the open research environment for fundamental research?

5. What good practices could be put into place by academic researchers to balance the open environment of fundamental research with the needs for national (and economic) security?

6. What good practices could be put into place by funding agencies such as NSF to balance the open environment of fundamental research with the needs for national (and economic) security?

To address these questions, JASON engaged with NSF leadership, senior university administrators, the intelligence community, and others. This report details the results from the ensuing inquiry, discussions, and debates engaged with NSF, senior university administrators, the intelligence community, law enforcement, and others.

Four main themes emerged from the study:

- The value of, and need for, foreign scientific talent in the United States,
- The significant negative impacts of placing new restrictions on access to fundamental research,
- The need to extend our notion of research integrity to include disclosures of commitments and potential conflicts of interest,
- The need for a common understanding between academia and U.S. government agencies about how to best protect U.S. interests in fundamental research while maintaining openness and successfully competing in the global marketplace for science talent.

Our Findings and Recommendations amplify these themes and propose steps the NSF can take to improve the security of fundamental research.

Findings

1. There is a long and illustrious history of foreign-born scientists and engineers training and working in the United States, and they make essential contributions to our preeminence in science, engineering and technology today. Maintaining that leading position will require that the United States continues to attract and retain the best science talent globally.

2. The United States upholds values of ethics in science, including objectivity, honesty, accountability, fairness and stewardship (NAS 2017 *Fostering Integrity in Research*). These values protect research integrity, upon which credibility of the fundamental research enterprise, and the entire academic system, is based.

3. Actions of the Chinese government and its institutions that are not in accord with U.S. values of science ethics have raised concerns about foreign influence in the U.S. academic sector. JASON reviewed classified and open-source evidence suggesting that there are problems with respect to research transparency, lack of reciprocity in collaborations and consortia, and reporting of commitments and potential conflicts of interest, related to these actions.

4. The scale and scope of the problem remain poorly defined, and academic leadership, faculty, and front-line government agencies lack a common understanding of foreign influence in U.S. fundamental research, the possible risks derived from it, and the possible detrimental effects of restrictions on it that might be enacted in response.

5. Conflicts of interest and commitment in the research enterprise can be broader than those that are strictly financial, including those that might occur in foreign research

collaborations or result from required reporting obligations for scholarships or grants.

6. There are many stakeholders with responsibility for the integrity of fundamental research, from U.S. government agencies to individual scholars, each with particular perspectives, roles and responsibilities. Universities and research funding agencies have policies and guidelines regarding some of these responsibilities, but these are often insufficient for individuals to assess risk and take appropriate actions.

7. National Security Decision Directive (NSDD) 189, established in 1985 a clear distinction between fundamental research and classified research. This remains a cornerstone to the fundamental-research enterprise, as officially reaffirmed in 2001 and 2010 and it continues to inform policy today.

8. Universities have mechanisms to handle Controlled Unclassified Information (CUI) under existing categories, such as HIPAA, FERPA, Export control, and Title XIII. CUI protection is difficult, but suited to these tasks, however it is ill-suited to the protection of fundamental research areas.

9. International researchers in the United States are partners in our research enterprise, and, consequently, in the effort to strengthen research integrity nationally and globally.

Recommendations

1. The scope of expectations under the umbrella of research integrity should be expanded to include full disclosure of commitments and actual or potential conflicts of interest.

2. Failures to disclose commitments and actual or potential conflicts of interest should be investigated and adjudicated by the relevant office of the NSF and by universities as presumptive violations of research integrity, with consequences similar to those currently in place for scientific misconduct.

3. NSF should take a lead in working with NSF-funded universities and other entities, as well as professional societies and publishers to ensure that the responsibilities of all stakeholders in maintaining research integrity are clearly stated, acknowledged, and adopted. Harmonization of these responsibilities with those of other federal research-funding agencies is encouraged.

4. NSF should adopt, and promulgate to all stakeholders, project assessment tools that facilitate an evaluation of risks to research integrity for research collaborations, and for all non-federal grants and research agreements.

5. Education and training in scientific ethics at universities and other institutions performing fundamental research should be expanded beyond traditional research integrity issues to include information and examples covering conflicts of interest and commitment.

6. NSF should support reaffirmation of the principles of NSDD-189, which make clear that fundamental research should remain unrestricted to the fullest extent possible, and should discourage the use of new CUI definitions as a mechanism to erect intermediate-level boundaries around fundamental research areas.

7. NSF should engage with intelligence agencies and law enforcement to communicate to academic leadership and faculty an evidence-based description of the scale and scope of problems posed by foreign influence in fundamental research, as well as to communicate to other government agencies the critical importance of foreign researchers and collaborations to U.S. fundamental research.

8. NSF should further engage with the community of foreign researchers in the United States to enlist them in the effort to foster openness and transparency in fundamental research, nationally and globally, as well as to benefit from their connections to identify, recruit and retain the best scientific talent to the United States.

9. NSF and other relevant U.S. government agencies should develop and implement a strategic plan for maintaining our competitiveness for the top science and engineering talent globally, taking advantage of new opportunities for engagement that might arise, even as others become more challenging.

Conclusion

JASON concludes that many of the problems of foreign influence that have been identified are ones that can be addressed within the framework of research integrity, and that the benefits of openness in research and of the inclusion of talented foreign researchers dictate against measures that would wall off particular areas of fundamental research. We expect that a reinvigorated commitment to U.S. standards of research integrity and the tradition of open science by all stakeholders will drive continued preeminence of the United States in science, engineering, and technology by attracting and retaining the world's best talent.

This Page Intentionally Left Blank

Appendix C APPROACHES OF OTHER AGENCIES: DEPARTMENT OF DEFENSE AND DEPARTMENT OF ENERGY

While JASON was undertaking this study, the DOD and the Department of Energy (DOE) were both working on their own efforts to identify unclassified domains of research that merit additional protections for national security reasons. JASON was briefed by these agencies on their approaches. We review these approaches here.

C.1 Department of Defense Approach: Researcher-Based Exclusion Lists

On June 29, 2023, the Office of the Under Secretary of Defense for Research and Engineering released the *Policy for Risk-Based Security Reviews of Fundamental Research* that is to be applied to *all* projects selected for funding. This review centers around a Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions.[50] In principle, the construction of this matrix recognizes both that international collaboration is "an important mechanism for participating in the global scientific commons and promoting progress in fundamental research" and the potential for foreign influence to result in the misappropriation of R&D efforts. In application, the risk matrix focuses specifically on identifying investigators with potential associations with a Foreign Country of Concern (FCOC), principally the People's Republic of China (PRC), with an aspirational goal of not substantially increasing the time to award and thereby delaying research progress. This matrix both identifies actions that would preclude an investigator or institution from receiving funding and describes conditions under which mitigation is required or recommended. As such, the Decision Matrix focuses on the *people* who would conduct the research and is agnostic to the research area.

At the top level, the DOD Decision Matrix, in alignment with §10632 of the CHIPS and Science Act, expressly excludes researchers who have participated in a malign foreign talent program, and those whose institutions do not have policies directly addressing malign foreign talent programs, from receiving DOD research funding. On the next-lower level of concern, the matrix identifies individuals who have other con-

[50] U.S. DOD, Under Secretary of Defense for Research and Engineering, "Countering Unwanted Influence in Department-Funded Research at Institutions of Higher Education," June 29, 2023, accessed December 21, 2023, https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF.

crete indicators of a conflict of commitment, including participation in other foreign talent recruitment programs, receipt of funding from an FCOC, a patent application history that is indicative of funding from an FCOC, or direct affiliation with an entity on the U.S. Bureau of Industry and Security (BIS) Entity List. Risk mitigations extend along a range of options, such as the removal or replacement of a co-principal investigator from a multi-investigator proposal, risk awareness training, and increased reporting frequency. Negotiations on these mitigations occur between the sponsor agency and the sponsored-projects office of the proposing institution, not the principal investigator (PI).

While the considerations listed above are relatively concrete indicators of previous or ongoing associations or affiliations with FCOCs, mitigation measures are also recommended or suggested for those who appear to have historical co-authorship with an individual who is now on the BIS Denied Persons List. While this is expressly *not* grounds for the rejection of a proposal, it will increase the burden associated with proceeding with the work, which may itself be a disincentive. Given that the the Entity and Denied Persons Lists contain more than 1,000 entries, the fraction of U.S. PIs who might be affected may be significant.

C.2 Department of Energy Approach: Critical Technology Identification

The DOE approach attempts to balance the protection of research results and intellectual property in a small number of identified technology areas with recognition of the importance of international collaboration to maintaining U.S. S&T competitiveness. As a result, it is constructed with the intent of continuing international S&T engagement with countries, including China, in a majority of research fields, while implementing restrictions in areas where its "scientific community assessed there was not a net-gain for U.S. interests and scientific progress." The DOE's Science and Technology Risk Matrix focuses on specific emerging technology topics associated with economic competitiveness, national security, or scientific leadership (e.g., quantum, batteries, AI); and on potential engagements with a specific country of risk, entities, or individuals (e.g., China, Russia, North Korea, and Iran).

Importantly, this approach strongly leverages the existing DOE laboratory research security environment and builds on existing DOE Integrated Safeguards and Security Management (ISSM). The effort is led by the 17 DOE National Laboratory Chief Research Officers. Subject matter experts are engaged to evaluate the current state of progress in each topic area and to create and update a categorization scheme as to which research developments constitute fundamental and non-sensitive insights

(Green), have the potential to be sensitive from an economic or national security standpoint (Yellow), or require additional protective measures (Red), as illustrated in Figure 6.[51] The Red category is meant to be a very select set of research areas, to minimize the overall impact of extra protections. This categorization guide is updated on an annual or more frequent basis to reflect developments in each field. Unlike the DOD approach, the matrix applies only to activities at the DOE National Laboratories (not universities). Further, it targets only the restriction of activities such as foreign engagements, cooperative R&D agreements, official travel, and foreign national engagement and access to the projects and data that involve countries of risk (China, Russia, Iran, and North Korea).

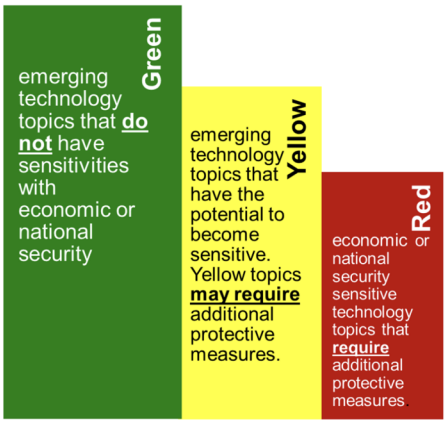

Figure 6: DOE approach to categorizing research security risk.

[51] U.S. DOE, Office of Science, slides from a presentation by Jeremy Ison at COGR Multi-Agency Panel on Research Security Risk Assessment & Analysis, October 26, 2026, accessed January 8, 2024, https://www.cogr.edu/sites/default/files/Multi-Agency%20Research%20Security%20Panel_0.pdf. [30]

This Page Intentionally Left Blank

Appendix D CONTROLLED UNCLASSIFIED INFORMATION

NSF tasked JASON with evaluating whether Controlled Unclassified Information (CUI), established by the Obama administration in 2009, could be a framework for identifying and protecting unclassified but sensitive research at academic institutions. JASON does not have legal expertise; but, as an understanding of CUI authorities and their limits is necessary to recommend a path forward, we review these here to best of our abilities. Earlier in this report, we discussed the federal origins of CUI in Section 2.3, commented on CUI as a basis for identifying sensitive research (Section 4.1), and commented on possible consequences of CUI designation (Section 5.3). We add additional information on CUI in this appendix.

D.1 CUI as a Basis for Identifying Technologies

JASON was asked "What existing structure and guidance for federal Controlled Unclassified Information (CUI) might be applicable to identifying NSF-funded research/technology areas of concern?"

The National Archives is the executive agent for CUI and operates the CUI Registry, the government-wide online repository for guidance regarding CUI policy and practice. The CUI Registry details specific categories of information the government protects and includes 18 organizational index groupings, such as critical infrastructure, defense, export control, financial, immigration, intelligence, international agreements, personal health information, proprietary business information, etc. JASON reviewed these but did not identify any existing CUI categories that would give NSF guidance for identifying technologies that need protection.

In general, technical information designated as CUI is protected because of its proprietary or physical-security nature. The one exception is technical information protected under export controls, which is a CUI category. Export controls exist for a wide range of political, economic, and national security reasons.[52] Export control law is complex and beyond JASON expertise; and export control lists are extensive, with ambiguities that often need to be resolved in the export-license review process. How-

[52]Michael Mastanduno, "The United States Defiant: Export Controls in the Postwar Era," *Daedalus*, vol. 120, no. 4, Fall 1991, pp. 91–112, accessed December 21, 2023, https://www.amacad.org/sites/default/files/daedalus/downloads/Daedalus_Fa91_Searching-for-Security-in-a-Global-Economy.pdf; Mario Daniels and John Krige, *Knowledge Regulation and National Security in Postwar America* (Chicago:University of Chicago Press, 2022). [1]

ever, we observe that, in general, export controls apply to high-Technology Readiness Level (TRL) technologies, usually artifacts, that have particular features specific to sensitive applications that are not themselves articulated in the export control lists. By contrast, fundamental research usually occurs at low TRLs, with notional but unproven applications (see Section 4.3). For this reason, the export control lists do not provide a foundation for identifying domains of fundamental research that merit extra control.

D.2 Does CUI Create an NSF Obligation to Control?

CUI was established by Executive Order 13556 in an attempt to unify protection standards applied by government agencies to a patchwork of sensitive information categories. The rules governing the implementation of CUI are codified in 32 Code of Federal Regulations (CFR) Section 2002. The protections that apply to CUI depend on the specific subcategory of CUI. Where specific controls are already specified in law, regulation, or government-wide policy, those pre-specified protection standards apply and are collectively categorized as *CUI-Specified* protections. Otherwise, *CUI-Basic* provisions outlined in 32 CFR 2002 apply. Although agencies may enhance CUI safeguards internally, §2002.22 prohibits such extra safeguards from being extended to entities outside of the agency absent a law, regulation, or government-wide policy specifically permitting this.

CUI-handling rules are not automatically binding on private entities that might obtain CUI-eligible data. To the extent that private entities are subject to CUI, that happens through contracts. 32 CFR 2002 encourages agencies to enter into written contracts with private organizations before "sharing" CUI with those entities. Those contracts are supposed to promulgate the safeguard provisions outlined in §2002.14, which apply to all kinds of CUI, whether *Basic* or *Specified*.[53] Only in this way do CUI controls become binding on private entities. Such contracts are logical for organizations that might, for example, conduct data processing on behalf of the U.S. Government. This limits the application of safeguards to the scope of the contract. For example, were CUI contracts used in a research setting, identical work occurring in the same laboratory, but funded by a nonprofit, would not be subject to CUI safeguards. Violations of contract provisions are but violations of the contract itself, with limited recourse unless other sanctions are defined in law.

Although this mechanism exists, the envisaged "sharing" conditions are quite differ-

[53] Agencies are technically allowed to furnish CUI data to private entities without contractual provisions in place if doing so serves the mission of the agency.

ent from what occurs in the course of fundamental research. In most fundamental research, NSF does not transfer any technical information (CUI or otherwise) to researchers. Rather, the concern here is that potentially sensitive information may be generated *de novo* in the course of research. Whether this creates an obligation upon NSF to insert CUI controls into the terms and conditions of its awards may depend, in part, on who owns the information being created in the course of research; and, in part, on whether CUI contracts can be applied to information that does not derive from government custody. These questions are discussed further in Section D.3.

D.3 Can NSF Use CUI to Create New Controls for Fundamental Research?

In order for an agency to create new CUI categories, the agency must have specific authorization to do so by law, regulation, or government-wide policy. We interpret Public Law 81-507 §15(b)(2) as potentially granting NSF the authority to create new CUI categories, although this interpretation should be reviewed by legal experts. If this authority exists, then the same question arises here as in the discussion above: Does NSF have the power to pre-designate information as CUI before its discovery in the course of fundamental research? Again, the answer may depend, in part, on who owns the information being created; and, in part, on whether CUI contracts can be applied to information that does not derive from government custody.

With respect to ownership, the terms and conditions of NSF awards convey information about the ownership of intellectual property in two ways: patent rights and copyright. In both cases, NSF awards generally leave those rights with the researcher but grant the U.S. Government a nonexclusive, nontransferable, irrevocable, paid-up license.[54] In this sense, the intellectual products of the research are not "work for hire," and NSF's ability to designate newly created information as CUI may be limited because CUI is established by executive order, and an executive order cannot regulate private property.[55] The type and/or terms of NSF awards may need to change (e.g., from grants to contracts) if NSF is set on using CUI provisions as a foundation for research controls.

[54]https://www.nsf.gov/pubs/2002/nsf02151/gpm7.jsp#731.3, https://www.nsf.gov/pubs/2002/nsf02151/gpm7.jsp#732.2.

[55]Limits to executive power have recently been re-litigated with respect to vaccine mandates. In all cases to date, the executive has lost. See Congressional Research Service, "Georgia: 2021 WL 5779939 at *12" and "Kentucky: 2021 WL5587446 at *13–14" in *State and Federal Autority to Mandate COVID-19 Vaccination*, May 17, 2022, accessed December 21, 2023, https://crsreports.congress.gov/product/pdf/R/R46745.

With respect to the authority, under CUI rules, to establish contracts protecting newly created information that does not derive from government-furnished information or a preexisting legally protected category, 32 CFR 2002 offers a variety of ambiguous interpretations.[56] A legal opinion is needed before determining whether CUI rules require or permit NSF to create contracts that extend CUI safeguards to not-yet-discovered fundamental research information.

It is unclear if the framework of CUI can provide a general vehicle for controlling fundamental research outside of government. At minimum, to use CUI for an NSF-designated technology area of concern would require that NSF create a regulation (see Section D.4). Whether the CUI information protection rules are substantively useful as a template for research controls is discussed in Section D.5.

D.4 Alternative Authorities to CUI

In general, there are two ways a government agency like NSF may regulate private activities: through a rulemaking process authorized in law, or by contractual terms. For example, academics handling medical records must comply with privacy standards specified by the U.S. Department of Health and Human Services (HHS). HHS obtains this authority to regulate private entities' handling of privately generated medical data through a law.[57] Similarly, if Census data is used for social-science research, that data must be protected under Title XIII of the U.S. Code. It is protected foremost because there is a law. However, in the case of Census data, the data are also designated as CUI, are owned by the government, and are obtained by researchers from the government. This means when the U.S. Census Bureau provides these data to private researchers, the Census Bureau is encouraged to enter into a contractual agreement with those researchers that would impose additional CUI-handling provisions on the researchers. (In practice, the Census Bureau protects such information by furnishing

[56] 32 CFR 2002.1(f), along with 2002.4(c) and 2002.16(a), clarifies that contracts with private entities to protect CUI are to be used when "agencies intend to share CUI with a non-executive branch entity." The language in these sections is suggestive of CUI that is already existing, and with information flowing from the government to private entities, not the reverse. At the same time, a strict reading of "share" could be interpreted to have a more bidirectional sense. Additionally, §2002.4(h) says "CUI does not include... information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency." This expressly articulates the possibility of CUI being created anew by outside entities on behalf of the government through a work-for-hire mechanism. However, later, paragraph (mm) appears to envisage private companies collecting extant CUI on the government's behalf, such as collecting social security numbers to process a loan application.

[57] U.S. Congress, *Health Insurance Portability and Accountabiity Act of 1996*, 104th Congress, Public Law 104-191, title II, §§261, 264(a)–(b), 110 Stat. 1936, 2021, 2033 (1996), accessed December 21, 2023, https://www.congress.gov/104/plaws/publ191/PLAW-104publ191.pdf.

researchers with Title XIII–qualified computer systems and Research Data Centers.[58])

In the law establishing NSF, Public Law 81-507, Section 15(b)(2) allows the Foundation to "establish security requirements and safeguards, including restrictions with respect to access to information and property, as it deems necessary." If this can be interpreted as a rulemaking authority in law, then NSF could go through a rulemaking process to identify domains of research that must be protected according to rules that NSF sees fit to impose. Rulemaking is, however, a slow and inflexible process. The procedures are set forth in the Administrative Procedure Act of the U.S. Code (5 USC 551 et seq.). Typically, an agency must give the public notice of a proposed rule before it goes into effect. Notice is accomplished by publishing the proposed rule in the Federal Register, and then the public is given an opportunity to submit comments on the proposed rule. The agency may take the comments into consideration before the final rule is published. In addition to the procedures outlined in the Act, there are a variety of other laws and executive orders that restrict regulations. In the case of NSF-sponsored research, the following may be relevant: If the proposed rule will have significant impact on small institutions, an additional defense of the economic impact is required (5 USC 603–614). Similarly, federal agencies cannot create rules that impose economic burdens on state government–funded institutions, such as state universities, without offsetting those costs (Executive Order 13132). Finally, if the rule can be construed as imposing limits on speech, additional defenses are required (Executive Order 12630). The final rule is then subject to actions by the President and by Congress before it goes into effect. Thus, if rulemaking is being considered, NSF should ensure whatever rules it puts forward are compatible with the rapidly changing states of knowledge in fundamental research domains. A rule governing the dissemination of information in a specific research sub-area, for example, could easily become obsolete by the time the rule is put in place. Rulemaking is also risky in that if a rule turns out to be harmful to academic competitiveness or to a specific discipline, or overtaken by events, it will take time and effort to remove it.

A more flexible alternative to rulemaking is to establish security mitigations and/or controls by the terms and conditions of the award. Such provisions can be adapted to suit the needs of each project and amended mid-stream, responding quickly to changes in the state of the art. These agreements do not create CUI. Over the course of this study, JASON did not become aware of any reason why NSF should favor rulemaking actions over customizing the terms and conditions of awards.

[58]U.S. Census Bureau, Data Stewardship Executive Policy Committee, "Policy on Controlling Non-Employee Access to Title 13 Data," 2009, accessed December 21, 2023, https://www2.census.gov/foia/ds_policies/ds006.pdf.

While there are many potential unintended consequences of implementing research controls (see Section 5.3), we highlight a particularly important one here: *Any* vehicle that imposes *access or dissemination* restrictions on information will *automatically* eliminate the Fundamental Research Exclusion (FRE) articulated in National Security Decision Directive (NSDD)-189. If such research, information, or technology falls into an export-controlled category, then even casual engagements with foreign nationals—such as research seminars, conferences, and eventually publication—could become deemed exports that are criminal actions. Publication of this material may require an export license. For these reasons, we urge NSF to use caution before imposing access or dissemination restriction on information stemming from research, and to do so in a narrowly scoped way.

D.5 CUI as a Template for Research Controls

NSF asked JASON, "What processes and restrictions might be implemented to carry out research that falls within the NSF-designated CUI category?" We interpret this more broadly to mean an NSF-designated domain of research requiring control.

To the extent that NSF might be looking to CUI as a template for research controls, we note that the CUI-Basic protections outlined in 32 CFR 2002 were not designed to protect national security–sensitive information, which might limit the utility. Specifically,

- CUI-Basic may be shared with foreign entities, 32 CFR 2002.16(a)(5)(iii); and
- CUI-Basic may be shared without a formal agreement, if doing so serves the mission, 32 CFR 2002.16(a)(5)(ii).

Adequate protection of national security–sensitive information would require the definition of a new CUI-Specified category defined by law, regulation, or government-wide policy. However, 32 CFR 2002.14 does not distinguish between CUI-Basic and CUI-Specified in requiring that all authorized holders of any type of CUI must:

- Establish controlled environments;
- Prevent unauthorized individuals from overhearing or observing CUI;
- Require direct control or physical barriers to CUI;
- Use only printers, copiers, and scanners that do not retain data;

- Delete electronic data in a method that makes the data irrecoverable; and
- Store, transmit, and process data only on information systems meeting the NIST SP 800-171 standard, which outlines 110 computer security provisions that must be satisfied.

These rules could be construed as a notional set of research controls, should NSF judge controls necessary. These controls constitute access controls, with supporting policies to prevent either (a) unintentional, or (b) intentional access to protected information.

Again, we note that any access control is largely incompatible with the mission of educational institutions. Such controls would disadvantage students involved with a controlled project by denying them the opportunity to engage in the free exchange of ideas, peer review, and practice at science communication. These activities are central to a student's education as scientist and engineer. As such, these controls could compromise the educational mission of universities and NSF, and their necessity should be weighed against this cost.

Such controls could additionally impede creativity and innovation in the protected sectors. President Reagan's NSDD-189 states that "an environment [with] the free exchange of ideas is a vital component" of academic research, and that such openness is therefore "an essential element in our physical and national security."[59] Slowing research in areas of national interest would impose a negative national security cost that must be weighed against the benefit of preventing controlled information from easily leaking to foreign nations; while realizing that if an adversarial peer country is determined to acquire the protected information, such controls are unlikely to stop them.

The supporting apparatus for access controls would impose significant cost on the conduct of research and reduce research funding efficiency. JASON received from NSF cost estimates for what the University of Oklahoma has spent to support such work, for example. A warehouse-type building for CUI experiments was estimated to have cost $2M, and a new office building with access control adequate for classified work cost $7M. Building construction costs are only about 10–20% of their life-cycle ownership costs, translating to roughly $1–2M per year for both buildings. Required security and compliance staff add cost of four full-time equivalent personnel, equating to another $1M per year. Thus, a medium to large ($1–3M/year) research program

[59] Office of the President of the United States, *National Policy on Transfer of Scientific, Technical and Engineering Information.* National Security Decision Directive 189. September 21, 1985, accessed December 21, 2023, https://catalog.archives.gov/id/6879779.

might incur security costs around $1–3M per year above the baseline research cost, roughly doubling the cost of carrying out that research. This would constitute a serious loss of research efficiency. Slowing research by half could easily allow countries like the People's Republic of China (PRC) to pull ahead in strategic fundamental research areas.

Appendix E ACRONYMS

AAU	American Association of Universities
AI	Artificial Intelligence
BIS	U.S. Bureau of Industry and Security
CFR	Code of Federal Regulations
CHIPS	Creating Helpful Incentives to Produce Semiconductors
CMI	Civil–Military Integration
COGR	Council on Governmental Relations
CRS	Congressional Research Service
CSET	Center for Security and Emerging Technology
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
CUI//SP-CTI	CUI Category: Specified Controlled Technical Information
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DOE	Department of Energy
EAR	Export Administration Regulations
ESA	European Space Agency
EU	European Union
FCOC	Foreign Country of Concern
FERPA	Family Educational Rights and Privacy Act
FRE	Fundamental Research Exclusion
GDP	Gross Domestic Product
GPS	Global Positioning System
GRFP	NSF Graduate Research Fellowship Program
HHS	U.S. Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IR	Infrared
ISSM	Integrated Safeguards and Security Management (DOE)
ITAR	International Traffic in Arms Regulations
LIDAR	Laser Imaging, Detection, and Ranging
MCF	Military–Civilian Fusion
ML	Machine Learning
MOE	Ministry of Education (PRC)
MOST	Ministry of Science and Technology (PRC)
NAS	National Academy of Sciences
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology

NSB	National Science Board
NSDD	National Security Decision Directive
NSF	National Science Foundation
NSPM	National Security Presidential Memorandum
NSTC	National Science and Technology Council
PhD	Doctor of Philosophy
PAPPG	NSF *Proposal & Award Policies & Procedures Guide*
PI	Principal Investigator
PPP	Purchasing Power Parity
PRC	Peoples' Republic of China
QED	Quantum Electrodynamics
R&D	Research and Development
RF	Radio Frequency
RSI-ISAO	Research Security and Integrity Information Sharing Analysis Organization
S&T	Science and Technology
SDI	Strategic Defense Initiative
SOW	Statement of Work
STEM	Science, Technology, Engineering, and Mathematics
TIP	NSF Directorate for Technology, Innovation, and Partnerships
TRL	Technology Readiness Level
U.S.	United States

The CHAIRMAN. Thank you, Mr. Dabbar.
Ms. Puglisi.

STATEMENT OF ANNA B. PUGLISI, VISITING FELLOW, HOOVER INSTITUTION, STANFORD UNIVERSITY

Ms. PUGLISI. Thank you, Chairman Lee, Ranking Member Heinrich, 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. As was mentioned, I am currently a Visiting Fellow at Stanford University's Hoover Institution and previously served as the National Counterintelligence Officer for East Asia. The views presented here though today are my own.

My testimony will address why the DOE labs are targeted by China, and then discuss research security and potential mitigation strategies. Lastly, I will offer some lessons learned that include that this is a U.S. problem, not just a Department of Energy problem. China's government has explicit efforts to exploit its diaspora. While this must be addressed and countered, the rights of persons of Chinese ethnicity in the U.S. must be protected. Finally, we can't protect what we don't have. We have to invest in the future.

The U.S. science and technology research enterprise, and especially the Department of Energy labs, set the global standard for discovery and innovation. Creating a climate to safeguard science will take a mindset change. Many in the research community see current policy changes as punitive. Because of this, it is important to discuss benefits of collaboration broadly, as they are not the same across the different stakeholders. An individual researcher can benefit from a specific collaboration because it brings them additional resources, prestige, or access to data or equipment, but it might not be to the benefit of the U.S. Government, national security, or the U.S. taxpayer. While China is not the only country that targets the Department of Energy labs, China's policies to target the Department of Energy complex are a deliberate state-sponsored strategy to save time and money. China uses non-traditional collectors—expert scientists, business people, and students—to acquire technology and technological know-how. Our current system is not designed to counter this kind of threat.

Current mitigation tools are tactical and narrow by design because they are crafted to mitigate behaviors with the assumption that the actor fully participates in a laws-based/rules-based system. They are basically designed for traditional counterintelligence threats that focus on intelligence officers, military end-use, and illegal activities. The protections in the CHIPS Act and NSPM-33, and as a result some of the individual programs that have been put in place by agencies, such as RTES and NSF SECURE Analytics, are a good start. However, in my written testimony, I provide some factors for consideration when determining access to the labs and funding decisions. Reviewing individual factors can help, but what we really need is a more comprehensive mitigation strategy. Piecemeal solutions will not have the desired outcomes.

I cover these three suggestions in more detail in my written testimony, but briefly I put forth the following elements that would make up a national level program. First is establishing a national

center for open-source information. This would provide detailed information at scale for our institutions and help them make informed decisions. Second would be to create a kind of pre-check for collaboration. It is important to establish an accepted framework of protections and make those clear—the standards, the norms, and expectations for visiting researchers, post-doctoral scientists, and students, and those that agree to those parameters have a fast-lane for collaborations. And finally, investing in the future—the investments we make or don't make today will impact our future competitiveness tomorrow.

So in conclusion, it is important to remember that China takes a holistic approach to development. It blurs civilian and military, private and public. This has deep implications for the DOE complex because it impacts the basis of entry for Chinese students and postdocs to U.S. labs. China's laws, which include the ability to compel citizens to share information, regardless of who owns it, also complicate the ability for individual researchers to act independently. So moving forward, I leave the Committee with the following thoughts. We really must decide what winning looks like, and this will take a comprehensive strategy. Extreme positions, such as closing our eyes or closing our doors, only benefit China. We either discredit all the efforts to address the problem or we deprive ourselves of the contributions of foreign-born students or scientists.

And China is not a neutral actor. And why does this matter? Because China intimidates and harshly silences its critics. This has only grown in the past few years, and places individuals in untenable situations. We do our foreign students and colleagues a disservice by not highlighting this behavior. So I want to thank the Committee again for continuing to discuss this issue. These issues will make us uncomfortable because they challenge assumptions and established norms. However, we as a nation have to have these conversations if we are going to protect and promote U.S. competitiveness.

Thank you.

[The prepared statement of Ms. Puglisi follows:]

Testimony before the Senate Committee on Energy and Natural Resources on "Examining Research Security Risks Posed by Foreign Nationals from Countries of Risk Working at the DOE's National Laboratories and Necessary Mitigation Steps"

Anna B. Puglisi
Visiting Fellow, Stanford University's Hoover Institution
20 February 2025

Chairman Lee, Ranking Member Heinrich, distinguished members of the Committee and staff, thank you for the opportunity to participate in today's hearing and address the committee on this very important topic. It is an honor to be here alongside the esteemed experts on this panel. I am currently a Visiting Fellow at Stanford University's Hoover Institution where I research S&T policy development, global technology competition and research security mitigation strategies. 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.

My testimony today will address why the DOE labs are targeted by China and then discuss research security and potential mitigation strategies. I will discuss how our systems differ, how China's institutions are tools of the state, and how the role of the state impacts and influences all aspects of China's S&T ecosystem including universities, state key labs and commercial entities. Lastly, I'll offer lessons learned, which include:

- This is not just a DOE problem but a U.S. problem. China's system is not the same as our own and it impacts our ability to protect our technology and innovation base. China takes a holistic approach to developing technology—blurring the lines between public, private, civilian and military.
    - Our current mitigation tools are not designed to counter an entirely different system.
- China's government has explicit efforts to exploit its diaspora—and as a result our innovation base. This must be addressed and countered.[i] At the same time, the rights of persons of Chinese ethnicity in the US must be protected despite this deliberate exploitation.
    - Beijing in many ways understands our societal tensions. China's statecraft is directed at them, exploiting identity politics by promoting any changes in U.S. policy as ethnic profiling. It offers a narrative that it is merely a proponent of "development" and science, as a way to divert attention from its own questionable behavior. This is a well-funded effort.[ii]
- We can't protect what we don't have.
    - Scientists–and innovation–will thrive with funding, lab space and freedom to answer hard questions. This is what makes the DOE labs such a tremendous

resource. Sustained funding over time for people and facilities are a key component of technology competition. The investments we make or don't make today will impact our ability to lead and compete tomorrow.

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

The U.S. science and technology research enterprise—and especially the Department of Energy (DOE), sets the standard for discovery and innovation excellence globally. DOE is key to U.S. technology competition and in my opinion an underappreciated resource. Through its labs and plants, the DOE builds a technically capable workforce that supports future discovery and industry. More importantly though, DOE's work is also a window into the priorities of the U.S. government.

Historically, collaborations and sharing of data, research and human capital across national borders has always been a U.S. strength. However, it also creates vulnerabilities in our innovation base and the DOE labs as some countries use these collaborations and exchanges to acquire know-how and talent through legal, illegal and extralegal means.

The world has changed since many of the mitigation tools in the toolbox—export controls, CFIUS, FARA and the discussions around how to treat basic research put forth in NSDD-189 were put in place[1]. More pointedly, what we have done in the past regarding research security is no longer working. While I still believe we must embrace open science, our assumption should not be that all collaboration is good until proven otherwise. Unfortunately, some governments have put in place policies and programs to exploit their diaspora and seek collaborations to meet their strategic goals.

Creating a climate to safeguard science will take a mindset change. Our current tools are tactical and narrow by design because they are crafted to mitigate behaviors with the assumption that the actor fully participates in a laws based, rules based system and more importantly plays by the same rules. We know this is not the case for China.

We must recognize that are we in a competition for talent and ideas. We also need to acknowledge that many in the research community see changes in research security as punitive. Even though the policy community has been discussing these issues for almost a decade and has put in motion a lot of new research security requirements, many in the research community still debate whether there is a problem and argue that many of the policies are xenophobic. Because of this it is important to introduce a discussion of benefits and push our research community to do so as well. The "benefit" of collaborations is not always the same across the different stakeholders. We must break it down into the following:

- Does the individual researcher benefit?
- Does the university, lab, business benefit?

[1] NSDD-189, published in 1985 makes the distinction between basic and classified research and is referenced in many discussions regarding research security (https://catalog.archives.gov/id/6879779). FARA is the foreign agents registration act. CFIUS is committee on foreign investment in the U.S.

- Does the U.S. government and taxpayer receive the benefit of the collaboration and investment?

Benefits can be topic and stakeholder specific. An individual researcher can benefit from a specific collaboration because it brings them additional resources, prestige, lower cost labor in their labs and access to data or research equipment. However, that collaboration may not benefit the institution they belong to or the government agency that funds the work because of the loss of data, ideas and potentially intellectual property. There are also potential long-term implications of that loss. Continued dialog is essential to bridge these gaps in understanding.

Countering China's actions will take a team effort. When I meet with researchers, I remind them that there is no free lunch. That is true here today as well if we want to compete with China.

- Researchers need support to find the next cure, new materials or build new military capability
- Agencies need resources to properly vet and protect investments
- There must be a cost on entities or individuals that exploit open collaboration.

Why the focus on China:

China's policies[2] to target the Department of Energy 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, advanced manufacturing and materials, often in the early stages of development. [iii]

China has demonstrated a willingness to flaunt global norms to reach its strategic goals and has put in place policies and programs that undermine the assumptions built into our system. These include: a fair and level playing field, transparency, reciprocity and market-driven competition.[iv] These actions have far-reaching implications for the future of our nation and our ability to compete. 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.

While China is not the only country that targets U.S. technology and the DOE complex, according to the 2023 Annual Threat Assessment[3] "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 the crosshairs given the depth and breadth of its mission. What is clear is the following:

- China has a whole of nation approach to acquiring technology and knowhow

---

[2] Please see 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.

[3] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

from around the world.

- China views technology as a national asset.
- China has stated that it wants to dominate in the industries of the future—AI, biotechnology, advanced manufacturing and materials. All areas the DOE labs are focused on.
- All parts of Chinese society – academia, private sector, government –and all aspects of the research ecosystem --technology R&D, economic development, military modernization are controlled by the Chinese Communist Party at varying levels.
- China targets unclassified R&D before it is placed into protected areas (e.g. export controls or classified programs).
- China pursues knowhow, processes, and methodologies that it can then apply to weaponize and commercialize technology at US expense.
- China sees its diaspora as a conduit for technology and technological knowhow.

Today's hearing is about the risk to the DOE labs posed by individuals from countries of concern. It is well documented[v] that foreign talent is key to China's technology acquisition strategy. China uses non-traditional collectors—expert scientists, businesspeople and students--to acquire technology and technological knowhow. 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 are related to military technology, we will fail. These non-traditional collectors are rarely in CI databases—they are not intelligence officers. Our current mitigation system is not designed to identify and counter them. The protections in the CHIPS act and NSPM-33, and as a result the individual programs put in place at agencies such as DOE and NSF are a good start, but it will take a comprehensive centralized effort to fully counter China's actions.

Moving forward we must be honest with ourselves, our researchers and the world. While there are a lot of discussions about "de-risking," sometimes you can't "get to yes" because of the sensitivity of topics or the affiliations of the institutions and people involved. This is because of the choices of a nation state that seeks to exploit our system and openness, not because of U.S. policy or actions. The U.S. and international science and engineering enterprise is put at risk when other governments seek to benefit from the global research system without upholding the tenets of research integrity and sharing equally.

There are actions we can take to better protect our investments, not only at DOE but across the U.S. research enterprise. Reviewing both access to the labs and funding decisions should address the following issues:

- Does the entity have foreign ownership or control?
- Are there criminal or regulatory issues related to the entity or individual?
- Will this collaboration or development create dependencies in supply chains?
- Will the individual have access to sensitive equipment, supplies or data?
- Does the individual have ties to malign foreign talent recruitment programs or other kinds of conflict of commitment?

- What kind of foreign funding sources are involved (both monetary and in-kind)?
- Are there concerning behaviors or obfuscation associated with patenting to include transferring information to foreign entities after filing, filing in a foreign country without the DOE collaborators etc.
- Are there ties to foreign entities or foreign collaborators on specified lists or with specified characteristics?

However, while reviewing these individual factors are important, a more comprehensive mitigation strategy is needed. I put forth the following elements as part of a national level program. Piecemeal solutions that are not at scale will not have the desired outcomes. While different agencies with different missions won't have the same risk threshold, all should start with the same level of information and make data-driven decisions.

Establish a National Center for open-source information. This national level resource would provide background information and help researchers, universities and national labs make informed decisions. This information center (center) should be part of the US government or an FFRDC, and interact with the IC, but not be a part of the IC. This center would be the connective tissue that enables a fuller understanding of technology developments and development networks, centers of excellence globally, and connections to malign actors. While there have been past and current efforts to do this, they are not sufficient and are not at scale.

"Precheck" For Collaboration: The U.S. and likeminded countries must create clear standards, norms, and expectations for visiting researchers, post-doctoral scientists and students. Working with our allies and like-minded countries is essential to protecting our respective innovation bases. Developing an international agreement—including verification mechanisms—will enable collaborations while guarding against the actions of nations that do not adhere to global norms. An accepted framework of protections will enable streamlined risk-management processes for collaborations among member countries, their institutions, and principal investigators—a kind of PreCheck lane for approval.[4]

Invest in the Future: Infrastructure and STEM talent. The United States and other liberal democracies must invest in their futures. Not all jobs of the future will require a university degree, but they will require more specialized training. We also must remember that innovation comes from doing the research—if we are not doing the research, we will not be innovative. Growing domestic talent and technical infrastructure so our scientists do not have to go to our strategic competitors to do their research will be essential. The investments we make or do not make will impact our future competitiveness and ability to grow our economy and sustain our military capabilities.

[4] For a more comprehensive discussion of this proposal please see: https://www.hoover.org/research/how-create-and-sustain-rd-leadership

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 takes a holistic approach to development, blurring what is civilian, what is military, what is private and what is public. This has deep implications for the DOE complex because it impacts the basis for entry of Chinese students and post-docs into U.S. labs. China's laws which include the ability to compel citizens to share information also complicates the ability for individual researchers to act independently. Existing export and visa policies that build their restrictions around affiliations with a military end-user but make exceptions for civilian uses have limited affect. To the Chinese leadership, every civilian use is also a potential military use.

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

- We must decide what winning looks like—this will take a comprehensive strategy.
- Extreme propositions, such as closing our eyes (laissez faire) or closing our doors, only benefit China. We either discredit all efforts to address the problem or deprive ourselves of the contributions of foreign-born scientists.
- China is not a neutral actor. Why does this matter? China intimidates and harshly silences its critics. This has only grown in the past few years and places individuals in untenable situations. We do our foreign students and colleagues a disservice by not highlighting China's actions.[vi]

In closing, 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 are to protect and promote U.S. competitiveness and future developments. These conversations will make us uncomfortable because they challenge assumptions and established norms. If we do not highlight and address China's policies we give credence to a system that undermines fairness, openness and human rights. Thank you.

---

[i] 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 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). US-China Economic and Security Review Commission, "2019 Annual Report to Congress" (November 2019).

[ii] 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年省级引进国外智利专项经费直项目分配明细表],
https://web.archive.org/web/20201112190122/http://webcache.googleusercontent.com/search?q=cache%3AKAaZ3LpEe4oJ%3Arst.hunan.gov.cn%2Frst%2Fxxgk%2Ftzgg%2F201802%2F9516964%2Ffiles%2Fe1c7ddd51dda49f6b70a6ad5ae9b0490.xls+&cd=3&hl=en&ct=clnk&gl=us

[iii] 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).

[iv] 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 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).

[v] 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.

[vi] Roth, Kenneth "China's Global Threat to Human Rights", Global Report 2020

The CHAIRMAN. Thank you.
Dr. Richmond.

STATEMENT OF HON. GERALDINE L. RICHMOND, PRESIDENTIAL CHAIR IN SCIENCE AND PROFESSOR OF CHEMISTRY, UNIVERSITY OF OREGON; FORMER UNDER SECRETARY FOR SCIENCE AND INNOVATION, U.S. DEPARTMENT OF ENERGY

Dr. RICHMOND. Thank you very much, Chairman Lee, Ranking Member Heinrich, and distinguished members of the Committee. Thank you for the 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—working in science for 50 years now—and researcher, and also a devoted educator, I understand the critical importance of talking about this topic for maintaining the nation's competitive edge in science and technology and ensuring that our research efforts remain secure and beneficial to the American public. And may I add, in these 50 years I have seen dramatic changes in how we have interacted with countries of concern like China. I have seen them change. I have seen the threats become even stronger, and they are as much of a concern to me now as they were when I was Under Secretary.

The United States has long been a global leader in scientific discovery and technological innovation. It is one of the reasons why we are able to attract the best and the brightest in the world. According to a 2024 report from the National Science Foundation, foreign-born workers make up 19 percent of the overall STEM workforce, as Senator Heinrich pointed out, and 60 percent of the doctoral level scientists and engineers in computer science and mathematics in the U.S. were born outside of this country. We are an open, innovative society. It is the key driver of our economic success. At the same time, I realize, as we had at the Department of Energy when I was there, the actions of certain foreign governments pose unacceptable risks to the scientific enterprise.

During my tenure on the National Science Board under President Trump and now recently as Under Secretary for Science and Innovation at the Department of Energy under Biden, I saw firsthand the growing threats to the U.S. leadership in science and technology. As this Committee well knows, the U.S. enterprise would not function without foreign-born scientists and engineers, but we also cannot afford to have things stolen from us—properties stolen from us by nefarious acts that threaten our U.S. economy and our national security. We must strike a careful balance if we are to protect national security interests without stifling the innovation that has long been our nation's greatest strength. During my time as Under Secretary, DOE and its 17 national laboratories worked diligently to achieve the balance by aggressively strengthening research security through rigorous background screening, expert controls, and collaboration policies to mitigate risks of intellectual property theft and undue foreign influence. For example, DOE developed a science and technology risk matrix, as noted, to protect emerging technologies, and it continues to be updated. This matrix provides a guidance to address potential concerns associated with

economic and international competitiveness by identifying the risks associated with a given topic and the resulting level of controls that are required.

DOE also developed a comprehensive and rigorous approach to research, technology, and economic security—what I will refer to as RTES policy, established new procedures for reviewing financial awards and loans, and created a new RTES office to continue to evolve DOE's enhanced due diligence process, engage with external stakeholders, and review DOE national lab agreements involving foreign entities. These actions were supported by security directives from Congress—thank you—and administrative actions by the National Security Presidential Memorandum, which was worked on both in the Trump Administration and the Biden Administration—NSPM-33. Together, these measures are helping the Department and its partners mitigate risks that malign foreign governments pose to our research ecosystem, supply chains, and intellectual property.

For most U.S. universities—research universities—the level of due diligence required by NSPM-33 and DOE's updated policies is a newer paradigm. I saw this when I was on the National Science Board and I have seen it now. Research universities serve a critical interface between government, industry, and academia, and since I am back in academia, I know this, going back to my home. That is why during my tenure as Under Secretary, DOE focused heavily on helping universities develop their own procedures for fostering secure, yet open scientific collaboration, and training researchers on best practices. I am proud of the way many university administrations have stepped up to this research security challenge, including my own at the University of Oregon. Security is in the DNA and the structure of our national laboratories. It has been historically at our national laboratories and in DOE. It has not been the case at universities. That's why it's so important for us to work with them.

So as this Committee is evaluating research security measures of the U.S. science and technology research enterprise, I have offered several recommendations that are important to consider. While I cannot speak to the status of DOE activities in my current capacity, I can assure the Committee that regardless of the Administration, the Department of Energy and its national laboratories take the responsibility to protect the scientific integrity of our nation's assets seriously. Thank you for the opportunity to appear before you today on this important issue, and I look forward to our discussion.

[The prepared statement of Dr. Richmond follows:]

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.

The CHAIRMAN. Thanks so much to all of you for your opening statements. We will now proceed to five-minute rounds of questions alternating between Republicans and Democrats, and I will begin that now.

Ms. Puglisi, I would like to start with you, if that's all right?

Last week, the New York Times published an article in which you were prominently featured. You were featured discussing how the CCP has used legal threats to intimidate American researchers, including yourself, in an effort to suppress research that exposes its influence operations. Now, if the CCP is brazen enough to do this, to try to pressure and influence American researchers, what does that say about the ability they have to exert pressure on Chinese nationals from the People's Republic of China working within U.S. national labs, and especially keeping in mind that those individuals, if they are residents of China, what does that say about their ability to have pressure brought to bear on them given that they are subject to Chinese laws that can compel them to cooperate with PRC intelligence-gathering operations?

Ms. PUGLISI. Thank you for that question, Senator.

I think, you know, it really highlights a disturbing trend, right? I believe that, you know, we have talked a lot about how the hope was that as we moved forward with engagement and collaborations that China would change, and its laws and rules and norms would become more like our own. Unfortunately, that is not the case. And so, I think, as I mentioned in my opening statement and in my written testimony, the importance of talking about this behavior, and that if we ignore the pressures that these scientists and students are under, we really do them a disservice and we do our own society a disservice because then we become more like them.

But it really, you know, I think, highlights as well that it's really hard, you know, for us to understand that kind of pressure and that we need to put in place those guidelines to both foster those collaborations, but also to protect that technology and to ensure that that does not happen.

The CHAIRMAN. But needless to say, the pressure that could be brought to bear on Chinese nationals at these labs is immense.

Ms. PUGLISI. Yes, it is. And I think it highlights, as we have seen over the past year, the articles and stories about extralegal behavior, not only for scientists, but on different campuses of, you know, China's actions.

The CHAIRMAN. Now, Mr. Dabbar, your testimony states that the Department of Energy under the Biden Administration restarted engagement with China to share U.S. energy technologies developed in our national labs. In at least one instance, in 2023, a Lawrence Berkeley National Lab scientist went to China, where he advised the Dean of the School of Energy, Power, and Engineering at—University, who also happens to be an affiliate of the foreign influence arm of the Chinese Communist Party on how best to construct an engineering lab for the school. Do you think U.S. national labs should be engaged in these efforts with our greatest global adversary, and should American taxpayers be funding such support that ends up benefiting our adversaries in this way?

Mr. DABBAR. No, Senator Lee, I don't think we should. They have been very clear that they want to dominate the tech space. And as

I listed in my testimony, there is a long series of technologies, including in energy, that were invented at the DOE national labs and invented by American companies that was stolen. And so, it is a long track record on this topic of much of which they are selling to the world was invented in America.

And so, I think we need to be much more cognizant of this topic, and I think more controls are needed on this, as I mentioned in my testimony.

The CHAIRMAN. So that's an expensive proposition, losing valuable research for which we have paid dearly, and having it go to our greatest geopolitical adversary isn't an ideal outcome. In fact, quite far from it. This can have devastating consequences.

Now, Section 436 of the Fiscal Year 2025 Intelligence Authorization Act, which barred foreign nationals from adversarial nations from accessing our national laboratories received unanimous approval from the Senate Select Committee on Intelligence, by a vote of 17 to 0, but it was blocked from the National Defense Authorization Act due to opposition from the former Chairman of this Committee. The provision included a waiver process allowing exceptions when the Secretary of Energy determined the national or economic security benefits outweighed the risks. Now, given these strong bipartisan concerns, would you support enacting similar safeguards to protect our most sensitive research while allowing for limited high-level exceptions?

Mr. DABBAR. I would, Senator. Obviously, it's a bipartisan topic. The way the current DOE order is written—that was done when I was Under Secretary—basically required sign-offs to have any Chinese interaction. I believe a lot of it was delegated down to lower levels, which basically opened the doors, as far as I could tell from my conversations with DOE. I think we need to potentially do exactly as the Intelligence Committee looked at, which is flip it. Instead of authorizing and sign-offs, is to do it the other way, where the base case is to ban that from adversarial nations, and to give waivers as required. I think that's a better way, given decades of Chinese infiltration and attempts.

The CHAIRMAN. Leaving the default at "on" is dangerous, in other words.

I see my time is expired. We will turn the time over to Senator Heinrich.

Senator HEINRICH. Thanks, Chairman.

Ms. Richmond, you and I have interacted at some of our nation's most cherished national labs, places like Los Alamos. Do you have thoughts on what the current dismissals at DOE and NNSA could mean for our national security in the long term, and in particular for workforce morale?

Dr. RICHMOND. Yes, Senator Heinrich. Thank you for that question.

I agree, and you know, I hope you all know how committed I was in my position and now with regards to national security and the concern of China stealing our most valuable assets. But these cuts, particularly in the security area, but also having to do with our energy infrastructure, the cuts there, too, give me even greater concern because they are immediate, because to be able to work at NNSA, but also to be able to handle classified information, requires

a tremendous amount of background checks, polygraphs. They ask all your neighbors, and so, my neighbors are sick of being asked for all these things I have done. But the point is that when we make these cuts, even if we say come on back after this weekend cut, what are the chances that we have increased the risk of someone being hired by China to come over and share what they have been doing? I, too, have been recruited. I got a letter not too long ago that was like, for one hour's work, I could take $40,000.

Senator HEINRICH. Yes.

Dr. RICHMOND. Now, you know, I don't have a mortgage to pay, but there are other people that do. So I just have to say that these cuts, and especially how they are going to impact the energy infrastructure——

Senator HEINRICH. Yes.

Dr. RICHMOND [continuing]. I think it's time for us to go to the new Administration and to Secretary Wright and ask what was the process to decide how to do that, to make these cuts, because the process that we have at the Department of Energy to make cuts—and we do make cuts of our federal employees—is based on budget priorities. When we develop our budgets, we set the priorities, and if your part of DOE does not fit into those priorities of the White House and also the Secretary of Energy, then you eliminate those people, but you do it in almost a two-year process while you develop this budget.

Senator HEINRICH. Yes.

Dr. RICHMOND. Because the priorities are changing all the time.

Senator HEINRICH. And one of the things that I think it's important to share with folks is that one of the—probably the leading red flag for someone being a risk with respect to recruitment is financial distress. So we just created a whole bunch of people with really important clearances, really important expertise, who are all under financial distress. We created a bunch of targets for the CCP. And I think, I just—I am aghast at how unthoughtfully this is all being carried out.

Mr. Dabbar, good to see you again. I want to ask you to sort of walk us through what currently happens—well, talk about how the intelligence officers at the labs, the lab directors, and then DOE intelligence coordinate and then what happens when they don't all line up and agree.

Mr. DABBAR. Yes, Senator. So obviously, this has been a big focus. There's a classified report from MITRE that's out there that has evaluated the details of that. I think that's kind of safe to say, and they have obviously had some recommendations on that particular topic.

In general, what happens is that the intelligence component of the DOE has local officers at each of the labs for counterintelligence. They will do the screening of employees, if people are traveling, interactions, grant security clearances. And so, they do that interaction as part of that intelligence component with the lab complex. In general, that works quite well. DOE's intel arm is quite well-integrated with that effort. And I think the biggest challenge on this is not the structure of it, but as I was mentioning, who has the approval, right, to allow this interaction to happen. I will give an example. I have been told many times that any lab employee

can actually do a recommendation and potentially, I have heard, even a sign-off on people coming to visit a lab.

And so, if there is a PRC citizen who is employed at the lab, they could recommend another PRC group coming from China to enter the lab. And if the authority has been delegated down to the lab, sometimes these things are happening at a higher rate than maybe some people at headquarters might like. And so, who has authority in the sign-off and the interaction of that, I think that's the core practical issue that probably deserves to be raised to a more senior level than has, I believe, been delegated.

Senator HEINRICH. If you have specific examples of that, I would appreciate if you would share them with this Committee.

Thanks.

The CHAIRMAN. Senator Cotton.

Senator COTTON. Thank you, Mr. Chairman.

From my work on the Intelligence Committee over the last 10 years, and now as Chairman, I can tell you this issue is of critical concern to me. Our national labs are where we develop some of the scientific research and capabilities that are the envy of the world, but they lack security measures. And I can say that it's not just me, it's many other members of the Intelligence Committee. Five members are on this Committee. There is a reason why we passed legislation last year, unanimously, that would have stopped scientists from China and Russia and even Iran and North Korea and Cuba from being in our labs.

Mr. Dabbar, do you know how many Chinese and Russian scientists were in our labs in the last Fiscal Year for which we have data?

Mr. DABBAR. If I have seen your past testimony, I think the number is around 8,000.

Senator COTTON. Eight thousand. Out of a total of how many? Do you know?

Mr. DABBAR. Well, total lab employees are probably——

Senator COTTON. No, total foreign visitors.

Mr. DABBAR. Oh, I am not certain about that.

Senator COTTON. Forty thousand. So one out of every five foreign scientists in an American national lab is Chinese or Russian. Do you know how many American scientists get to go to equivalent sites in China and Russia?

Do you know, Mr.——

Mr. DABBAR. I think it's less.

[Laughter.]

Senator COTTON. If I put the over/under at 0.5, would you bet the over or the under?

Mr. DABBAR. Maybe even under.

Senator COTTON. Ms. Puglisi, how many American scientists get to go to the equivalent sites in Russia and China?

Ms. PUGLISI. Senator, I currently don't have that number. However, I think that's a point that I have made before this Committee and others is that it's not reciprocity. I mean, true collaboration comes from transparency and reciprocity. And that's one of the things that we are not seeing.

Senator COTTON. I couldn't agree more.

Ms. Richmond, do you think one out of every five foreign scientists at a Chinese or Russian equivalent site is American?

Dr. RICHMOND. I don't know those numbers, I'm sorry——

Senator COTTON. Yes, there is zero reciprocity on this issue. Why would we allow Chinese and Russian scientists into our national labs, to say nothing of Iranians and Cubans and North Koreans, when they don't allow our scientists there? We have told the directors of these labs for a long time, the Intelligence Committee, that if they do not get a hold of this problem then the Congress will solve it for them. And the legislation that we introduced and passed through the Intelligence Committee last year, although it didn't get passed into law, will be brought back up this year. And I am going to champion that on this Committee and on the Intelligence Committee because we have to put an end to this threat.

There are a lot of great people working in the Department of Energy, to include at our labs and at the Office of Intelligence and Counterintelligence, one of the very best of our small intelligence offices around the government, but there are too many people that have this "open science" mindset, this naïve ideological commitment that we have to allow these foreign adversary scientists into our labs, no matter what the risk.

Mr. Dabbar, who has the final word on allowing such a foreign visitor to visit his or her lab?

Mr. DABBAR. So the order is flexible on who has the authority. Previously, when we instituted it, when I was Under Secretary, it was required to be up at my level, and we were able to squash a lot of the thousand talents programs. We found many, many people working for China, including joint nuclear weapons work. That's a pretty stunning comment I just gave that we found at one of the labs. I believe—I was told in my conversations with DOE recently that a lot of that has been delegated down to the individual lab level, and I am not exactly certain——

Senator COTTON. And again, we have great people working at our individual labs, but by and large, the directors of these places tend to come from a scientific background, is that correct?

Mr. DABBAR. Yes, sir.

Senator COTTON. They are not coming from the intelligence community. They are not coming from law enforcement.

If a foreign national is excluded from one lab, is he therefore excluded from every other lab?

Mr. DABBAR. I am not certain how it's currently being executed.

Senator COTTON. I think the answer is no.

Mr. DABBAR. Yes.

Senator COTTON. If one of our lab directors says no, this guy from Russia is too dangerous a risk and can't be here, he can just turn around and try to go to one of the other labs as well.

Is it fair to say that sometimes there is a little bit of competition between these labs for money or prestige or talent?

Mr. DABBAR. Senator, in one of my times, one of my many times of uncovering things with intelligence, counterintelligence at the labs, we found a Chinese national who had been hired at one of the DOE labs and then they used that to shift to NIST in Colorado and use the—of having been hired at a DOE national lab to join a very important quantum effort at NIST. And as soon as we found that

out, we had to reach out to Commerce very quickly and point out that we were sorry that this person had gotten that role and basically, we allowed them to end up at another lab.

Senator COTTON. Thank you.

I just want to thank the Chairman for having this hearing. This is not something that we discuss much in a public setting. We have examined it very closely for years on the Intelligence Committee. But it is a grave national security threat. It is a threat to our prosperity as well because so much of these technologies end up getting commercialized. And to be clear, what we are talking about here, again, is foreign nationals. There has been a lot of testimony, or a lot of statements from members and the witnesses about the history throughout American life of foreign-born, naturalized scientists. We are not talking about that. We are not talking about someone who has raised their hand and taken the oath of affirmation to become a citizen or even a legal permanent resident. We are talking about foreign nationals coming to our lab. This is a grave threat and we can't allow it to continue.

The CHAIRMAN. Thank you.

Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman.

Good to have all our guests, and especially good to be able to welcome Dr. Geri Richmond, who is a long-time expert in security and also a long-time University of Oregon Duck, and we welcome you.

Dr. RICHMOND. Go Ducks.

Senator WYDEN. Let me, if I might, ask you about what we learned at DOE in the Pacific Northwest here very recently. There were abrupt and significant workforce reductions last week in the office that carries out the critical work to keep our electric grid reliable. My take is that this raises national security issues. It raises fundamental issues for our economy. What are the implications of something like that, Dr. Richmond?

Dr. RICHMOND. Well, thank you, Senator Wyden, it's good to be here with you too.

I think that in terms of our power, our energy infrastructure, and particularly the cuts at BPA, as well as the 1,800 people that were just cut off at the Department of Energy with no clear understanding of the procedure, or why, it really is going to—I believe as a citizen, that it's going to not only compromise the safety of our grid, but also will drive up energy prices. I believe that it will delay current projects in communities and that it will disrupt our supply chains. These are, again, my personal opinions, having served as the Under Secretary for three years, but I think it also is sowing confusion and chaos among the federal workers because they are learning about things in the news, and I can't confirm what's in the news either. But the point is that it's just leading to a lot of confusion.

For example, with BPA, there were a number of employees that were cut. And as a Pacific Northwesterner, like you, that's really chilling because BPA is so important.

Senator WYDEN. Let me see if I can get a couple of other questions in real quickly.

When you went through the process of getting your security clearance, did you have to disclose all of your foreign financial conflicts of interest and contacts with government officials?

Dr. RICHMOND. Yes. In fact, because I have worked in so many different countries—over two dozen developing countries, in particular—I had to list all the countries I had been to, whether they had paid for my travel support—which most of them did not—whether I had any kind of a conflict of interest with them, with any type of financial support from them continuing, what all my finances are with regards to all of the investments that we have. We had to declare all those. We had to be cleared for a general counsel. I had to get a polygraph test.

Senator WYDEN. I think I got the drift.

Dr. RICHMOND. Okay.

Senator WYDEN. If a U.S. Government official had significant business dealings with the government of China or failed to disclose all of these contacts with Chinese government officials, could that derail their access to sensitive Department of Energy secrets or classified information?

Dr. RICHMOND. Yes, and in fact what happened in the laboratories, during my time, was you had both the IN and also the lab leaders talking about when there is a concern about a person being in the laboratory. And what they go through is, who is going to come onsite, what is their background, what kind of access would be controlled if they did come onsite, and this is for visitors also, and what projects can they work on, and what partnerships do they have? If there is a disagreement between those two entities in the laboratory, then it gets sent up to me. I did not have any concerning ones that came up to me. And the laboratory said this at the HSST hearing, the director said this last week.

Senator WYDEN. Thank you, Dr. Richmond.

Colleagues, I am asking these questions for several reasons, and one of them is, according to public reporting, Mr. Elon Musk is running DOGE while remaining Tesla's largest shareholder. And according to that public reporting, Tesla has invested billions in China and makes one million cars a year at a factory in Shanghai on land owned by the Chinese government. Finally, according to public reporting, Tesla's contract allows the Chinese government to revoke Tesla's lease on the land at any time if it determines doing so is in the public interest. Now, on this Committee, every one of us works for the American public interest, and given that as our highest priority, I intend, colleagues, to come back and ask further questions about this in the days ahead.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Wyden.

Senator McCormick.

Senator MCCORMICK. Thank you, Mr. Chairman. Thank you to our panel. Grateful to the witnesses for coming to discuss such an important issue for our national security, but also for Pennsylvania. Pittsburgh is the home of the National Energy Technology Laboratory. Many employees from the Princeton Plasma Physics Laboratory commute across the Delaware River to call Pennsylvania home. And we must ensure that this critical national research and these wonderful assets are secure from foreign adver-

saries, and that America remains the global leader on energy and other advanced technologies.

So I really share the concerns raised by so many today about the continued theft of American research and innovation by the Communist Chinese Party. It is a huge national security risk for all the reasons we have talked about, but it's also the stated goal to dominate the commanding heights of technology and to use that technological supremacy to undermine America's economic might, its geopolitical position, our very way of life, and that research and technology theft is a well-documented key pillar of the CCP strategy. So with forced technology transfers, IP thefts, scientific espionage, not only providing the CCP with advantages in economic and environmentally important technologies, it's also undercutting American workers in Pennsylvania and in other places. We are essentially paying for the R&D that China steals to beat us in the market space. How can American companies compete in that environment?

So let me start with you, Ms. Puglisi. You pointed out that because the CCP does not play by the same rules in science and technology, that our often-narrow research security tools are outmatched by China's efforts to steal American technology and know-how. How can we make the jump from piecemeal solutions, some of which we have discussed here, to a national strategy for mitigating these threats?

Ms. PUGLISI. Thank you, Senator, for that question.

I think it's important to highlight, first, and the reason why—what creates this challenge is China takes a very hybrid approach. It takes a very holistic approach to its S&T development. And so, oftentimes, you know, we try to separate things out into complete buckets. And so, to have a national approach, what we need to do is recognize how different this system is, and to look at the individuals and the companies that we are dealing with holistically, and acknowledge those ties to the Chinese government, and in moving forward, how policies that are across both our infrastructure and in commerce that recognize that these are supported, that they oftentimes don't have to make market-based decisions, that individuals—and we know this—are sent to study here, to work in the laboratories for a purpose. And we just have to be much more deliberate about the way we look at people's backgrounds. And to begin with, I think putting in place very clear guidelines, because, you know, our system has been built on trust, right? And I have been in the lab. I have worked in the lab, and no one wants to believe that their collaborator is stealing their technology or the student that they are supporting is doing that or has some other alternative motives.

And so, we must make it very clear.

Senator MCCORMICK. And yet, we know they are.

Ms. PUGLISI. Yes.

Senator MCCORMICK. In many cases they are.

Ms. PUGLISI. And unfortunately, this has been the case, and it is well documented. I know the other witnesses have talked about this. I, myself, have written a lot about this. And so, I think the starting point is being very clear—what are those assumptions that we are making?

Senator MCCORMICK. Yes.

Ms. PUGLISI. And you know, sometimes we can't get to yes with some of these collaborations.

Senator MCCORMICK. Yes.

Ms. PUGLISI. And that's why we have to engage, you know, with the research community to really make clear on that and——

Senator MCCORMICK. Thank you. I am going to just move on to one more question here if I can.

Ms. PUGLISI. Okay, sorry.

Senator MCCORMICK. Thank you.

Ms. PUGLISI. Yes.

Senator MCCORMICK. Mr. Dabbar, good to see you again.

Many research institutions, just following up on this question, including the national labs, are engaging in research collaboration with third parties—I don't think we have talked about that much—here in the United States and overseas, and those third parties can also be exploited by our adversaries to steal sensitive research, particularly the CCP. What policies should DOE put in place to ensure that the research collaborations and joint research projects that may be outside the labs don't create additional security vulnerabilities? What authorities and directives can Congress use to help on that mission?

Mr. DABBAR. So that certainly happens. Let me give you an example. We do accelerator technology with our European friends, where they ship us some accelerators sometimes and we ship them some equipment sometimes. We generate IP in some of these very large pieces of equipment that could have dual-use points, and sometimes the Chinese go into Germany, to a lab in Germany, to try to appropriate IP that we invented at one of our national labs. I know that happened. I have specific examples of that. So I do think of any of our collaborations with our allies, we need to push the ball. I think we have pushed a ball of awareness of them in Germany, France, and whatnot, that China is trying to steal stuff, and that if they want to work with us, and if we are going to share technology with them, they have to meet the same sort of standards that we have for ourselves.

Senator MCCORMICK. So I think it's fair to say, regardless of how tight our security is in our own labs, if we have third party research efforts underway that are not equally strong in the security measures, then there is a back door where some of the same challenges of IP theft and so forth can occur.

Mr. DABBAR. Absolutely, Senator. I will pick on one thing that Senator Risch has been doing on fusion. America is about to break some major bounds on fusion in this next four years. There is going to be some major examples. They are trying to steal it from us and our international collaborations on fusion. And so, that's something that historically was more open science, and I think very clearly both domestically as well as international, that needs to be greatly enhanced since we are about to accomplish quite a bit.

Senator MCCORMICK. Thank you.

The CHAIRMAN. Senator Gallego, you are up next.

Senator GALLEGO. Thank you, Mr. Chairman. Perfect timing. And thank you to our Ranking Member, also.

Our national and energy security should always be, of course, top-of-mind. And I was proud to be a leader in passing the Fiscal Year 2025 NDAA. Among many other things, that bill enhanced vetting and limited the entrance of certain foreign nationals to DOE lab facilities to protect national security. But as former Chairman of the House Armed Services Subcommittee on Intelligence and Special Operations, I also know exactly how important it is to be deliberate in the way we discuss sensitive operations, especially in open settings. As we do our duty to oversee national labs in this Committee, we must not give away information that our adversaries could use against us or actively gather.

So I have a couple questions for Dr. Richmond. In United States military operations, our armed forces work with interpreters and local allies who make our operations more secure and successful. I certainly experienced that in Iraq in combat with local nationals, as well as foreign nationals, and third-party companies. And so, we have talked a lot about the risks of foreign infiltration in our DOE labs. Can you expand on the risks of siloing ourselves too much and missing vital information from our allies and foreign-born scientists?

Dr. RICHMOND. Yes, thank you, Senator, and thank you for your service also.

I think that we cannot closet ourselves. I have to say that before the wall came down in Europe, I was actually in East Germany and I got to see—it was weeks before the wall came down—and I could see what a closeted country looks like and I have also done the same in Cuba. We have to rely on intelligence from other countries too. We have to decide whether we trust it or not. We have to decide what we are going to do with it. But I am going to go back to your comments, ma'am, because we need a coordinated effort across all agencies and universities if we are going to use what intelligence we have in order to move forward. And the armed forces play a critical role in that, and as you know, if we did not have that outside information, those partners with us, it would be tough to go forward.

Senator GALLEGO. And even along the kind of siloing of information and sharing of information, from my experience, kind of, as the past Chairman of Intel/Special Operations, I even had complaints from our Five Eyes nations, people that we are supposed to share our most intricate and sophisticated intelligence with, that we still are in such a silo that we couldn't really share our intel across platforms fast enough for them to actually use it as actual intelligence. When it comes to sharing with our close Five Eyes partners or other intelligence treaty nations, do you see that also still being a problem in terms of some of the research that's found in maybe the UK, for example, not being as quickly transferable or easily shared for us to actually consume, use, or effectively continue the research on?

Dr. RICHMOND. Well, I think it's important—thank you for that question. I think it's important for us to add to this conversation this issue of open science. Open science is science that's going to end up in literature, it's going to be published together. That kind of collaboration happens at the laboratory because it's natural to do that, whether it be in fields like I have worked in with lasers and

optics and other fields too. We have to have that open science. So what I fear is the discussion of really restricting the labs to even things in personnel, even things that are truly open science, then my concerns are there. So I don't know if that went to your question, but it's a point I feel is really important for this Committee, many who are not scientists, to understand what the open science is as opposed to something that is truly an economic threat to us.

Senator GALLEGO. And your testimony outlines multiple measures, including a risk matrix to protect emerging research and tech at DOE. Are you also concerned that any of those security measures will be disrupted or dismantled under new agency leadership that does not really understand the goal and intent of that matrix?

Dr. RICHMOND. As a citizen myself, yes, I am concerned because when you have—what we have always found, and when I have gone into the SCIF—and we are not going to divulge any classified information—first of all, we do have people from other countries that are helping us in the intelligence for some of these countries. But the point is that we really have to be able to go forward in a manner that allows us to share the information that we need and be able to go forward. I am not sure if that quite went to your point.

Senator GALLEGO. Thank you. I yield back.

The CHAIRMAN. Senator Risch.

Senator RISCH. Thank you, Mr. Chairman. Thank you for holding this meeting. Look, this is a really, really important issue that gets almost no attention. I have been 17 years on both the Foreign Relations Committee and the Intel Committee, and we have watched this cancer grow over those years, and it's not going away. It's getting worse and worse. So I am going to start at 50,000 feet and bring this down. In 1983, I traveled in China. I left China thinking, you know, we are never going to have to worry about this. They had no plumbing. They had no toilets. They had no phones. They had nothing. It smelled. It was terrible. That was in 1983. If you go there today, it's like America. Now, it took us over 200 years to get where we are. And it has taken them only a handful of decades to get where they are. Are they that much smarter than we are? We all know better than that. They stole every good idea that we have, except for democracy and respect for human rights.

So how did that happen? Well, it happened because America is so open and so free that we just open the flood gates. And today, this problem of the people coming into the labs is joined with the question of people that come into the colleges and universities. They are identical problems, and the numbers are stunning. Americans have no idea that there are hundreds—hundreds of thousands of Chinese students studying in America, and we have a tiny fraction of that. And as Tom Cotton pointed out—he went and dug out the figures—of the thousands of Chinese people who visited our labs, and zero Americans have visited their labs. I am intimately familiar with the INL, of course, you know, the birthplace of nuclear energy on the planet. And I talk to those people all the time. I have never met a person who has set foot in a Chinese laboratory.

So this is the problem—we have given away the farm. And I would disagree with Ms. Richmond about open science. We should never have given them that, but that ship has sailed. The open

science is there. It's all over the internet. It's everyplace. But they have used it to bootstrap themselves up where they are.

So let's change lanes for just a second and talk about who we are dealing with. A student who comes here, or for that matter, an engineer who comes here and goes to one of the labs, may have no malign ideas whatsoever. But for a person who lives in a communist, autocratic country, nothing belongs to them. Their property doesn't belong to them, their thinking doesn't belong to them, their intellectual knowledge doesn't belong to them. It belongs to the Chinese Communist Party, because in those states, the state doesn't exist for the people as it does in a democracy like we have, people exist for the state, and the state always comes ahead of the people. And so, they take these people—when the students go home, they are debriefed by the Chinese Communist Party, and every scintilla of information they have then belongs to the Chinese Communist Party.

And I mean, it's two different systems. There is absolutely no question about it. But again, it's really time to slam the door on this thing. I have preached about this for years. And with all due respect to the scientific community, I can't get it through their head that this is a national security issue. They say, well, we are all on this planet together. The knowledge we have helps everybody. Well, yeah, to a degree. If we are fighting polio, that's true. But not when we are designing quantum computers. It's not like that at all. And we shouldn't be sharing that information at all.

So, and by the way, I get real pushback from the colleges and universities. Why? There are millions of dollars being transferred from China to the colleges and universities. And those colleges and universities get very defensive of the grants and that that they get from the Chinese Communist Party.

Anyway, that's where we are. Folks, how do we get the word out to the community, and how do we get the word out to Americans that this is a huge problem? And I have only got a few minutes left. Start down here and give me your 30-second take on that.

Ms. PUGLISI. Okay, thank you, Senator.

First, I just want to add that the whole issue of basic science comes up quite a bit, but it's important to note that collaborations are very important, and I, myself, have been a proponent for open science. However, I think what is lost in that conversation is that not everything is shared. And that is the challenge because what is happening is that the time and resource-intensive parts of that basic research, oftentimes, the data, the know-how, the access to how do I actually do something, and oftentimes what doesn't work is what is stolen. And so, those are the kinds of things, I think, that we really need to focus on and have that conversation.

Senator RISCH. Ms. Richmond, I am almost out of—I am out of time—give me a short shot and I am going to give you——

Dr. RICHMOND. Yes, let me say, I am glad to meet you. I have been through Chinese laboratories, back in 2010.

Senator RISCH. I have met somebody, finally. All right.

[Laughter.]

Senator RISCH. I have met one. How many people in America, 330 million? All right, I've got one.

Dr. RICHMOND. Yes. But the point is, things are changing——

Senator RISCH. By the way, did you get into the Wuhan lab, because we are really interested——

[Laughter.]

Senator RISCH. Probably not.

Dr. RICHMOND. You know, I can't read Chinese, so I have no idea what lab I was in. Okay?

But the point is, you raise a very important point. Things are changing. Your issue about the open science is right, but on the other hand collaborations are really important too. But again, I believe that we need to have a full discussion of this out in the open. Universities need to—and faculty at universities need to understand that they could be involved in the areas of high-performance computing, AI, quantum, bioscience, biotech, accelerator science, battery science, that we at the labs consider to be extraordinarily high-risk, so that they can understand that they are——

Senator RISCH. You got that exactly right.

Dr. RICHMOND. Yes.

Senator RISCH. Paul.

Mr. DABBAR. Senator, I think this is a big but narrow topic. America is the bright light to recruit people from all around the world who want to work at the DOE national labs and people want to become Americans. And I think that's good. When I was there, we had four lab directors who were naturalized citizens from the UK and Canada and Germany and so on, and that is excellent, right? They came here. They became American citizens. We are still a very small percentage of the world in terms of population in the big scheme of things, and I think doing that, and all the other people underneath them, with citizens from all over. China is the topic——

Senator RISCH. China is a problem because those people can't stay here. We all know what happens to their families if they say, hey, we are giving up China, and we are going to become a U.S. citizen. They will start—well, anyway, I don't want to go into that. They do bad, bad things to their families.

So my time is up. Thank you.

The CHAIRMAN. Thank you.

Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. I appreciate the panel discussion today. It's good to see some of you again.

Let me start off with the Nevada National Security Site. Most people don't have it in their backyard. I do. Most people don't grow up next to it. I did. Most people don't have family and friends that work there. I have and still do. So this is an issue that is important for us in Nevada, and I appreciate the conversation today.

Dr. Richmond, let me start with you. In your testimony you outlined various legislation like the CHIPS and Science Act and the Fiscal Year 2025 National Defense Authorization Act that address research security concerns that we have talked about, right, that are getting ready to go into effect. Specifically, though, you mentioned that DOE was getting prepared to implement Section 3112 of the NDAA, which would ban foreign nationals from China, Russia, North Korea, and Iran from accessing the national laboratories operated by the National Nuclear Security Administration without secretarial waivers. So given the enhanced research security meas-

ures outlined in the Fiscal Year 2025 NDAA, how do you think these new regulations will affect the mission at Nevada's national laboratories, such as the Nevada National Security Site, which we know is essential for maintaining our nation's nuclear weapons stockpile.

Dr. RICHMOND. Well, thank you, Senator, for that question. As you may know, Director Hruby—Jill Hruby—was the one that oversaw NNSA while I was in my position, so I don't have all the depth of knowledge that she would have, but I do think that the lab directors that spoke last week at HSST, even Dr. Kim Budil was there, and she does oversee Lawrence Livermore National Laboratory. And all five directors that were there—three or four of them were NNSA labs—they are ready to do it and have accepted it and we will have it done by April 15 or whatever the deadline is.

Senator CORTEZ MASTO. Okay.

Dr. RICHMOND. What impact that has, I can't speculate on it, but I think they are ready to take it on. The concern is, though, that they are now going to have to fire, I think, a number of people. I think it was close to a thousand or something like that, and that, again, compromises our security because those people could easily be picked up by our adversaries.

Senator CORTEZ MASTO. Can I touch on that, because I only have so much time, and that was my next question because we are now implementing legislation to address foreign nationals coming into our labs, but what we are not doing is addressing the workforce that is necessary. Now, I have heard all of you, and we have had this conversation before about STEM, making sure our kids are exposed to it, that they want to go into that area of science. We want to make sure that they are now stepping into, as they graduate, jobs like we have at the test site. What does it say to them that we have just done this wholesale firing of people, particularly in my state. People are paying attention—their family members, their friends, they know what is going on. What does that say to our ability to develop that workforce for the future in these STEM courses?

Dr. RICHMOND. Okay, I will put my academic hat on now. People are scared. Students are scared. Parents of students are scared. Spouses are scared about paying mortgages, that all the energy that they have put into this passion they have for science is now being questioned for its value. It's very personal.

Senator CORTEZ MASTO. Let me touch on one final thing. We have talked about foreign nationals, and I agree that we have to address it. We have passed legislation to do just that, but there are other security challenges we are not even talking about—cyber threats. Where are we talking about cyber threats here? And should we be addressing that as Congress as well?

And let me open it up to any of the panel members: talk to me about cyber threats. What should we know that we are not talking about today that is the next step for us to implement when it comes to our national labs?

Ms. Puglisi or Mr. Dabbar.

Ms. PUGLISI. That's a very important point and that's why I advocate that we really need a holistic, comprehensive program that

looks across the board, and cyber would be one of those, and also, both external and internal to understand, okay, who's sharing what with whom. So that's one. And I just want to pull the thread on the collaborations because that's an important point and why we really need to demand that reciprocity and transparency because it can't be a one-way street, right? And we talked about how many people are in our labs, how many people in their labs, I mean, these are serious topics and serious countries do serious things. And so, we need to ensure that there is that reciprocity of, not only people, but information. And one of the challenges, I think, with China is they are coming down on open science—access to their data, access to academic papers, you know, that does not demonstrate to me a place that has a serious desire to do true collaborations.

Senator CORTEZ MASTO. Thank you.

I know my time is up. Mr. Dabbar, do you have anything?

Mr. DABBAR. So Senator, this is a university example, but not a lab example. This just goes to show you that you need to have strict controls, and sometimes things can go wrong. We found a cybersecurity effort that was funded by DOE at a university in which all the principal investigators were PRC nationals. Electric grid cybersecurity funded by DOE at a university with PRC nationals developing the software for cybersecurity for the electric grid. We stopped that as soon as we found out that that had been done, and I won't go through the details, but it's an example that people were not thinking, okay, at the Department, when they were issuing funding of something that I think is pretty commonsense.

So I think this comes back to rules and proper oversight so that people down below don't do things that wouldn't pass, you know, kind of commonsense for, I think, anyone in this room.

Senator CORTEZ MASTO. But if we don't have the staff to catch it. Thank you.

The CHAIRMAN. Senator King.

Senator KING. Thank you, Mr. Chairman.

The focus today has been on national security, as well it should be. That's one of our jobs around here. On the other hand, there is an opportunity cost of excluding talent that could be important in furthering our own interest in terms of technological development.

Ms. Richmond, talk to me about that. It seems to me what we really need to do is try to find a path between total exclusion and not being cognizant of national security risk, but not exclude people who can make a significant contribution to our national welfare. Do you see what I am trying to find?

Dr. RICHMOND. Yes, so, Senator King, thank you for that question. There are so many examples of where Chinese citizens have made—I would be happy to give the Committee many examples, especially of Chinese researchers who continue to contribute in our laboratories and also our universities. It is a balance. And particularly for our universities, we have, while I was Under Secretary, we started the RTES Office, which is Research for Technology and Economic Security. And that is basically to make sure that we don't have things happen like happened in your Administration, which would check every one that's a PI going in for a grant. In

the FOA that goes out, it is checked to make sure that it is very clear that we are going to ask this kind of information when you apply for a grant. Then, when the selections are made, look to see who the PIs are, are they ones that are safe to go forward with? Is the topic one—what about the topic, because the security for some topics——

Senator KING. But universities don't have the security clearance apparatus——

Dr. RICHMOND. No.

Senator KING [continuing]. That the national labs have.

I believe that there may be more risk, frankly, on the university level than there is at the national labs because at the national labs you have a whole—you have counterintelligence at Department of Energy and you have those kinds of examinations.

Dr. RICHMOND. And that's why we are working with them and that's why we are sharing the risk matrix with them as well. I was on a video call recently to talk about what they need to do in proposals with their PIs to give them guidance on making——

Senator KING. Mr. Dabbar, how do you think we should strike this balance?

Mr. DABBAR. Yes, so, one of the orders that we also implemented was banning giving money to university researchers if they were also taking money under the Thousand Talents Program. We had found out that during the previous Administration, that they had allowed that, so that literally a researcher could be getting money from the Chinese state at the same time as from DOE. We decided that was a bad idea. We actually spent a bunch of time with university presidents explaining that. They had a lot of worry about that. And then, at the end of the day, they reached a conclusion that the Federal Government can decide what to do its money. I know it's a simple kind of conclusion.

But one of the big things that they found, as a part of our pushing on this topic, was they found out that they had researchers who were spending significant time in Communist China and basically taking their research—it had nothing to do with DOE, it could have been from anyplace. And they didn't even know it was happening. I found out at Stanford, for example, there was a professor who was supposedly full time, who spent nine months a year in China. And the university didn't even realize it was going on, even though they were paying that professor.

So I think awareness with the university system, that they need to address their own problems, but I do think additional controls around how the Federal Government money is given to PIs, the principal investigators——

Senator KING. Let's go back to the national labs.

Mr. DABBAR. Yes.

Senator KING. If there is a total ban, no Chinese researchers whatsoever, is that a good policy or would that cost us some good scientific breakthroughs that would otherwise be useful? I am trying to find the right line between national security and opportunity cost of brilliant researchers from anywhere in the world.

Mr. DABBAR. I think, Senator, given that there has been, literally, a whole generation of successful efforts by Communist China in stealing stuff, the Los Alamos Club, but then the thou-

sand talents. They keep coming at us. I think the better way of doing it is this proposed legislation from the Intel Committee that was referenced, which is a ban with Chinese nationals at the national labs, which are at the very highest level of the United States with the ability of the Department of do a waiver. And so, this flexibility——

Senator KING. So the default would be no.

Mr. DABBAR. The default should be no, is my recommendation, which was the Intel Committee's unanimous vote, with the ability of the Department to grant waivers. So there is still flexibility in the idea, but once again, I think the DOE national labs are at the top of the security worries.

Senator KING. I understand.

Quick follow-up question. Who is Chinese? There are a lot of Chinese Americans. Are they swept into this? What's the definition?

Mr. DABBAR. Yes, so the way the orders are written is, it's citizens.

Senator KING. Chinese citizens.

Mr. DABBAR. Citizens.

Senator KING. Okay, so a Chinese American who has been here 50 years or a couple of generations would not be included?

Mr. DABBAR. Citizens is the way that the order is currently written.

Senator KING. Okay, thank you.

Mr. DABBAR. Or Russians, or, I mean, we had an Iranian trying to get hired, like an Iranian citizen, and we had concerns on the type of technology and we decided not to let them in.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Senator CASSIDY [presiding]. Thank you.

And I have taken the gavel, just for everybody's information, while Senator Lee goes to vote.

Let me follow up on that. I don't know the particulars of it, but by the way, I have been elsewhere, so if I ask something which is a repeat, I apologize, but I am going to pick up where Senator King left off. There were two folks who apparently were American citizens, but who were passing information to the Chinese Communist Party, that were recently arrested from the DOD. And I want to say it's out in San Diego. I am a little vague on all of this, but suffice it to say that this occurred. So if the restriction is on Chinese citizens, and by the way, I am Irish American, right? So I am not saying we have this kind of prohibition upon Chinese Americans. I am trying to understand this kind of interface where there has been an infusion of people who now are naturalized U.S. citizens, but in some way still might pose a security risk.

And so, we want fairness. We want to capitalize upon incredible human talent, but we don't want to be someone's sucker. So take into account these naturalized citizens, and how would we do that, as a follow up to what Senator King asked in terms of establishing security?

Yes, ma'am, would you like to go?

Dr. RICHMOND. Yes, so, I think that's a really good question. So we have, just to put some data out there, of the Chinese citizenship at graduation. After they have been here for five years, 88 percent

have stayed, and after ten years, 81 percent have stayed. So some—I mean, a lot of them are going to stay. And the question is, which ones are the ones that you need to be concerned about? So I think what we have done with working with the universities and NSF and certainly, Paul, with your administration work on this too, is the Department of Energy, back in 2019, and then 2021, every PI, every one that wants money, has to put down all their connections, okay? And with regards to money, visits, financial support, all of that has to be there if you are going to get DOE money.

And I have been in the SCIF where I have been talking to our intelligence people about someone that may arise that causes them concern. And those people are also working with our vetting—RTES group—in order to figure out who those people are because they—I tell university PIs that if you don't disclose, and we find out that something is wrong, you are out of here.

Senator CASSIDY. So let me ask you this, though, because I once read about how the Chinese missile program began because there was a Chinese American who was doing fabulous work, but because of a security issue, was not given clearance to continue and he just wanted an outlet for his intellect. And so, he returned to Communist China and helped develop their program. So I guess that brings to mind, is there a way to discern between those people who are more loyal to China and those who are more loyal to the United States, but if we shut off opportunity, they will go where they have opportunity. Do you follow where I am going there?

Dr. RICHMOND. Well, Senator Cassidy, that's exactly what we have been talking about here, is the concern about all the cuts that are happening in the Department of Energy—300 employees at NNSA, 1,800 across the Department, and those people have an incredible knowledge, scientific background, and if they are just really upset, shall I say, they may decide to do that. So it concerns me that——

Senator CASSIDY. Well, people have got to eat. So they have got to have a job.

Dr. RICHMOND. Yes, you have to pay the mortgage. You have to eat. You can take that contract that I, you know, asked that I—the letter that I got recently that said $40,000 for an hour's worth of work in China. We will pay all your expenses. And you know, for somebody that is mad, is angry at the government or for——

Senator CASSIDY. But that's not actually, that's not my fundamental question though. I am going back to this person in the 1940s or 50s who was really seeking opportunity. So is there a way to discern between those who might be a security risk and those who are, you know, they are just, they may leave, but they are going to leave because of opportunity or other circumstances, not because of their security risk, fundamentally?

Dr. RICHMOND. So in the case of the people, again, we go through with the RTES program and also the risk matrix at the laboratories, we go through as much information as we can that they will give us with regards to when they are employed at the university or, excuse me, employed in the Federal Government to find out whether they could possibly be a risk.

Senator CASSIDY. And of course, this would apply to people of multiple nationalities. I think I heard you mention as I walked in,

because there are talented people coming into the United States for graduate school from the world over, right?

Dr. RICHMOND. Yes, but you don't have to only worry about if someone has Chinese background.

Senator CASSIDY. I get that.

Dr. RICHMOND. There are American scientists that have decided they needed the money so they went over to China.

Senator CASSIDY. I am a little suspicious about some of the Canadians——

[Laughter.]

Dr. RICHMOND. I don't know, I think it's Irish Americans we need to worry about.

[Laughter.]

Senator CASSIDY. You don't have to worry about Irish Americans for much.

Senator Hickenlooper.

Senator HICKENLOOPER. Thank you, Mr. Chairman, and thanks to all of you for being here. I appreciate this. I grew up in a time back in the 60s, where at the height of the Cold War there was a continuing cartoon series in Mad Magazine where it was Spy vs. Spy, and there was a white spy and a black spy, and they were constantly doing tricks with each other in a comical competition. We are way beyond that. And I think, you know, when I was just getting—I got a master's in earth and environmental science, and we had a number of foreign students within our program, and it was embryonic in that sense of how much they added from their educational system to things that we didn't emphasize or didn't understand as well and vice versa. I got a great appreciation with that.

I taught field geology for a year down in Costa Rica while I was still a graduate student and saw that culture and got those exchanges. It's incredibly powerful. I mean, look at the number of our largest companies that have been started by immigrants. The amazing innovations and breakthroughs that have come from people that came to this country because they wanted to live in a free country. To be quite honest, that magnet is still very powerful.

But I want to ask each of you, I mean, are we doing enough? Is the current system sufficient to protect our classified research from foreign espionage?

Mr. DABBAR. So Senator, I do think, as we have been discussing, I think a heightened level of awareness because there has been generation after generation of Chinese just adapting to try to steal. I would make a broadening point to your question, which is not just classified, I mean, the leading renewables lab in the world is in your state. It's not even close, okay? No other country comes close to that.

And so, just to pick on a topic: perovskites for thin-film solar may be the next big thing. We don't want that to be in Xinjiang, produced by coal and slaves, literally slaves, right, because they are the wrong religion. I thought we were over that in 1945, but the Chinese are doing that.

Senator HICKENLOOPER. Right.

Mr. DABBAR. And I am certain they are trying to steal it from your lab—or your nation's lab.

Senator HICKENLOOPER. I view it as my lab.

Mr. DABBAR. Yeah, yeah—in your state.

And so, I think as a broadening point—not just classified—it includes both economic impact technologies as well as classified.

Senator HICKENLOOPER. I would agree.

Dr. Richmond.

Dr. RICHMOND. Yes, I agree with that. And I think what we are talking about here is an evolving situation, and it will continue to evolve. So we have to have a system together that is adaptable, can quickly move——

Senator HICKENLOOPER. But is our system now sufficient, is the question, right? We have got to be adaptable, but there are all kinds of things we can do to improve it, but——

Dr. RICHMOND. It can always be improved. It can always be improved, but I think, certainly under the Biden Administration, we took what we got from the past administration, heightened it up even more. And as we go through, we are going to have to look to see how much it needs to be heightened any more.

Senator HICKENLOOPER. That's fair.

Dr. RICHMOND. But again, it's not just classified information. It's also the AI and many of the other areas.

Ms. PUGLISI. And I am going to foot-stomp that. It's beyond—it's more than the classified information because it's really a lot of the technologies of the future—it's AI, it's biotech, it's the new materials in manufacturing. And so, I think what is really important is to focus on the behavior. And I think that a lot of the new regulations and rules that are being put in place are a start and are beginning to do that, but I think it's going to take time to implement those. And again, I think we have to take that really holistic look. And we can't set and forget, right? This is dynamic. The technology is changing. The vectors—the threat vectors are changing. And so, it's going to require a constant dialogue.

Senator HICKENLOOPER. The magnitude of those threat vectors has never been greater.

Ms. PUGLISI. Right.

Senator HICKENLOOPER. And I think we have to maintain that sense of urgency that you guys all have shown.

Ms. PUGLISI. Yes.

Senator HICKENLOOPER. So I appreciate that.

Several of you have talked about foreigners coming into our universities and being more motivated or adding a great deal to innovation. I think we have got to get back, also, to how do we get our kids in this country—I mean, the reason universities are receiving and open to receiving these foreign students is because we don't have a pipeline that is sufficient to provide the technology and the STEM kids. We have got to get to them in elementary school. Do you guys have, do you realize—do you connect that problem and the solution of it with this issue about our national security?

Start at this end, this side.

Ms. PUGLISI. That's an excellent point. I mean, STEM education, we should start at K–12 and really do things to support——

Senator HICKENLOOPER. K–3.

Ms. PUGLISI. Yes, actually, the earlier parts, I mean, because you hear kids, by the time they are in middle school, they are saying——

Senator HICKENLOOPER. Absolutely.

Ms. PUGLISI [continuing]. I can't do math.

But that's going to take an effort, and we want to make sure that we draw from the wide swath of Americans from all over the country. And so, that starts, you know, with support from the undergraduate and make people understand what the possible is and also, I want to—it's the technically proficient workforce——

Senator HICKENLOOPER. We are out of time.

Dr. RICHMOND. So do you realize that our country has the lowest retention rate in the world for kids that decide they want to be a scientist at 18 and don't end up being a scientist at 24?

Senator HICKENLOOPER. Outrageous. I totally—I do know——

Dr. RICHMOND. Lowest.

Senator HICKENLOOPER. Outrageous.

Senator CASSIDY. Senator Justice.

Senator JUSTICE [presiding]. Oh, thank you so much, Mr. Chairman.

You know, I have said this a bunch of times, but I am probably a new kid on the block, but I am not a kid, you know, I have got a lot of white hair and I have been around, and around, and around. I can tell you just simply just this—I truly believe that energy, absolutely, is the key to just about every single thing that we have got going. That's all there is to it.

Now, and if it's that level of key, I have just got to share with you just a couple things, real quick. First of all, we have one of these 17 labs in Morgantown, West Virginia, and we are really proud of that. And I can tell you that I have just gotten through being the Governor of the great State of West Virginia for eight years, and to be perfectly honest, we were able to do lots and lots and lots of good stuff. And little West Virginia, that a lot of people told a lot of bad jokes about, to tell you the truth, along the way, became a diamond in the rough that everybody missed. And with all that being said, successes like you can't imagine. And we are really, really proud of exactly what we did.

Now, with that being said, along the way, there was a gentleman that I ran into way, way, way before I ever became Governor, and he was a PRC national and just the most legitimate-speaking gentleman that you could ever be around. And then, all of a sudden, as I became the Governor, we found out things that were going on with him in his life and everything that tied right back to his homeland that absolutely astounded us. I mean, absolutely a gentleman that—as a guy that is suspicious of almost everybody a lot of times, but absolutely trusting in everybody—I believed with all in me that this guy was the real deal. A guy that absolutely we trusted in every way. And we were astounded with what we found. That's all there is to it.

Now, energy is, I think, so important it's off the chart right now. It's off the chart how important energy is. Do you realize if you are a business guy—and that's me—do you realize that we can't cut our way out of these messes? We can't. We can mind the store and we can surely do a lot better, but at the end of the day, we got to

find a way to grow. And the way to grow, absolutely, hands down, is energy, period. That's all there is to it.

So if it is the most important—and it is, it truly is, you know—then we have got to be on guard and we have got to do better because the world is trying to absolutely discover or steal our innermost secrets all the time—all the time. So with all that being said, I would say to everybody, from the guy that's the white-haired guy from West Virginia that's a business guy, not a politician—I am a guy that talks to you just with common sense and logic. I would say beware. And absolutely, we got to do better. And these folks right here are the key to us doing better in a lot of ways.

So I do have one question, and it just parallels everything that I have already said because, you see, I really believe that President Trump, because I am a real friend with the family, and I am proud of that, and absolutely, I am trusting of the family, and he is our President and he is now saying to all of us, look, we have got a problem here. We need to do better. And so, let's get at doing better. But my question real fast is just this, and this is to Ms.—is it Puglisi? Did I get that halfway close?

Ms. PUGLISI. Puglisi, yes.

Senator JUSTICE. Okay, you know, and my question is just this, given your expertise in counterintelligence or research security, can you provide insight into the extent of collaboration between DOE national laboratories and the Seven Sons universities in China, please?

Ms. PUGLISI. Thank you very much.

Well, I, myself, have not done empirical research to be able to give you the exact numbers. There have been a number of articles that look at those kinds of collaborations. And for those who are not aware, the Seven Sons are universities that work directly with the military. And so, you know, this is very concerning because, you know, China says that it will—it's civil military fusion. It will use anything that it acquires and apply it to its military. And so, those are affiliations and collaborations that we really need to take a closer look at.

Senator JUSTICE. Well, thank you so much. And I know my time is expired, but I would say just this—I will do anything and everything I can do to help all of you in every way at any time. We have got to become safer and we have got to become more protective, in my book.

Thank you so much.

The CHAIRMAN [presiding]. I want to thank all of our witnesses for being here today. This really has been a great hearing, and we are going to keep the record open until close of business, 6:00 p.m., tomorrow, February 21, for the submission of written questions for the record for our witnesses and items included in the hearing record.

I do, before we gavel out, I want to just correct the record on some things that have been said today.

Over the last week there has been a lot of fairly misleading and poorly sourced reporting regarding dismissals at the U.S. Department of Energy, and here are some facts that I think are relevant and significant, but often omitted. President Trump and the Department of Energy are committed to making government more ac-

countable, efficient, and restoring proper stewardship of the American taxpayer dollar. And the previous Administration was not a responsible steward of that, and we are paying the price for it heavily in the form of inflation. In just four years, the Biden Administration expanded the Department of Energy's federal workforce, and it did so by more than 20 percent, adding more than 3,000 federal employee positions. In the last year alone, the Biden Administration increased the size of the Department of Energy federal workforce with 1,000 new employees.

Delivering on President Trump's mandate, supported by more than 77 million American voters, the Energy Department began on Thursday dismissing a portion of recently hired federal employees classified in the Federal Government as probationary employees. Across the Energy Department, less than 700 probationary employees have been dismissed. These dismissal numbers pale in comparison to the total amount of positions the Biden Administration hired over the last four years. They are also less than the total positions added by the Biden Administration in the last year.

Now, contrary to many news reports, the Energy Department's nuclear weapons production plants and nuclear laboratories are exempt from these dismissals. So those aren't part of it. At the Energy Department's Power Marketing Administration, PMA, fewer than three percent of total employees were dismissed and were primarily administrative roles. Of the more than 70,000 contractors and federal employees at the National Nuclear Security Administration, or NNSA, fewer than 50 employees were dismissed. These employees held primarily administrative and clerical roles. The Energy Department will continue its critical mission of protecting our national security and nuclear deterrents in the development, modernization, and stewardship of America's atomic weapons enterprise, including the peaceful use of nuclear technology and non-proliferation.

So it is important that we keep the facts aligned. When people are crying that the sky is falling, it usually is not, and that certainly is the case here. In any event, I thank the witnesses for being here today. It has been a good, informative discussion. We have laid a good record and I very much appreciate your help.

The hearing stands adjourned.

[Whereupon, at 11:44 a.m. the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

ANSWERS TO

QUESTIONS FOR THE RECORD

BY

THE HONORABLE PAUL M. DABBAR

FORMER UNDER SECRETARY FOR SCIENCE

U.S. DEPARTMENT OF ENERGY

ADJUNCT SENIOR RESEARCH SCHOLAR, CENTER ON GLOBAL ENERGY POLICY, COLUMBIA UNIVERSITY

CO-FOUNDER, BOHR QUANTUM TECHNOLOGY

BEFORE THE SENATE ENERGY AND NATURAL RESOURCES COMMITTEE

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

HEARING DATE: FEBRUARY 20, 2025

Questions from Senator Steve Daines

Question 1: Mr. Dabbar, we are witnessing a historic shift in the global landscape of STEM innovation and education. Since 2007, China has outpaced U.S. universities in producing STEM doctorates. What role should the Department of Energy's National Laboratories have in fostering domestic talent and supporting American graduates to remain competitive in this evolving landscape?

Dabbar Answer: DOE, as well as the other STEM university granting agencies (such as NASA, NSF and DOD) contribute significantly to developing graduates. Students who work on research supported by these grants become the next generation of talent. The Senate could provide additional support for that in the various agencies' authorizations and appropriations. In the last four years, inflation adjusted support for this has dropped, leading to reduced support for talent development.

Question 2: Mr. Dabbar, our 17 DOE National Labs lead the way in scientific innovation, conducting both basic and applied research that fuels economic growth and advances cutting-edge technologies. Among them, five labs host National Quantum Information Science Research Centers, which are pushing the boundaries of quantum computing, communication, sensing, and materials. These efforts promise to transform fields like science, energy, security, communication, medicine, finance, and logistics. However, some of these labs are open to international collaboration, which makes them potentially vulnerable to adversarial nations. This exposes U.S. technological leadership to risks, as intellectual property becomes increasingly threatened. How can the Department of Energy effectively integrate the DOE S&T Risk Matrix to assess and categorize risks in quantum technology research and development, ensuring the protection of intellectual property, addressing quantum supply chain challenges, and reducing barriers to commercialization?

Dabbar Answer: The DOE S&T Risk Matrix includes restrictions on quantum research collaborations with people citizens of the countries of risk. While it is good to include participation from allied nations in their non-classified quantum R&D, citizens from adversary nations should be restricted. The Senate could consider statutory full bans of collaboration with citizens from countries risk on any quantum related topic, to eliminate any risk that an administration could waive the matrix requirements.

Question 3: Mr. Dabbar, Lawrence Berkeley National Lab is home to one of the five National Quantum Information Science Research Centers, specifically the Quantum Systems Accelerator. This center is driving national leadership in quantum information science and technology by co-designing the algorithms, quantum devices, and engineering solutions necessary to achieve certified quantum advantage in DOE scientific applications. However, this same laboratory has also been linked to researchers affiliated with Chinese government talent programs, which U.S. authorities have identified as tools used by the Chinese Communist Party to acquire foreign technology and intellectual property. How can the Department of Energy ensure robust protection of our quantum technology intellectual property, enabling our National Labs to advance research and development efforts that address supply chain challenges and reduce barriers to commercialization?

Dabbar Answer: DOE and the National Labs such as LBNL need to be both offensive on quantum strategy, i.e. support additional R&D, as well as defensive, i.e. ensure what we develop is not appropriated by adversary nations.

The Labs, and universities supported by DOE, should get additional support for this highly important frontier technology. Also, they should be allowed to collaborate with researchers from allied nations, some of whom are also advancing strongly in the area. And we should increase support for both start-up and larger companies that are taking these discoveries to market.

In addition, applied quantum efforts are advanced enough to develop first generation highly effective quantum computers. I would recommend that DOE start the next-generation High Performance Computer program promptly, that would include quantum chips in the design.

On the defensive side, DOE should look at implementing a blanket ban, subject to waivers if appropriate, from citizens of countries of risk from doing any work at or with National Labs in this area.

Questions from Senator Cindy Hyde-Smith

Question 1: In 2022, Strider Intel published "The Los Alamos Club" report which gained broad U.S. and international media coverage. This report uncovered how China, for more than 20 years, had infiltrated programs within Los Alamos National Laboratory, stealing research and key information from numerous programs including hypersonics research. This massive infiltration by the CCP talent program allowed individuals, after years of working at Los Alamos, to return to China and start similar programs that resulted in massive loss of technological advantage for the United States and associated national security implications. Congress remains concerned about Chinese success at infiltrating our National Laboratories gaining access to advanced research and intellectual property that threatens U.S. technological and economic advantage, and our national security. In 2022, these efforts were illuminated in the highly publicized "The Los Alamos Club" report that highlighted CCP talent program infiltration at Los Alamos National Laboratory spanning decades. This is not a new problem.

1) What steps has the Department of Energy and the National Labs taken, including commercially available open-source intelligence tools, to identify and mitigate the security risks posed by foreign nationals from Countries of Risk working at, or in collaboration, with the DoE National Labs?

Dabbar Answer: DOE has many tools to identify security risks at the National Labs, including classified sources from various intelligence community components. And during the Trump Administration a series of public orders were issued to eliminate this sort of espionage and technology appropriation. However, since these steps were solely at the discretion of DOE, including implementation of this policy by politcals, recent enforcement has been lessened. While the orders significantly reduced the risks, in the recent years, DOE approved significant re-introduction of PRC citizens into the labs, as well as direct engagement with PRC government officials in-person in China around re-starting sharing our energy technology invention.

The Senate could consider the ban, unanimously approved by the Select Committee on Intelligence, of all countries of risk citizens at all the National Labs, only allowing entry subject to a waiver. The Senate could consider mandating that only Under Secretaries or above could provide that waiver, and mandate those waivers to be in writing. The Senate could also consider applying a similar ban on any sort of engagement with countries of risk, also subject to a similar waiver process.

U.S. Senate Committee on Energy and Natural Resources
February 20, 2025 Hearing: ***Research Security Risks Posed by Foreign Nationals from Countries of Risk Working at The Department of Energy's National Laboratories and Necessary Mitigation Steps***
Questions for the Record Submitted to the Honorable Geraldine L. Richmond

Questions from Senator Cindy Hyde-Smith

Question 1: In 2022, Strider Intel published "The Los Alamos Club" report which gained broad U.S. and international media coverage. This report uncovered how China, for more than 20 years, had infiltrated programs within Los Alamos National Laboratory, stealing research and key information from numerous programs including hypersonics research. This massive infiltration by the CCP talent program allowed individuals, after years of working at Los Alamos, to return to China and start similar programs that resulted in massive loss of technological advantage for the United States and associated national security implications. Congress remains concerned about Chinese success at infiltrating our National Laboratories gaining access to advanced research and intellectual property that threatens U.S. technological and economic advantage, and our national security. In 2022, these efforts were illuminated in the highly publicized "The Los Alamos Club" report that highlighted CCP talent program infiltration at Los Alamos National Laboratory spanning decades. This is not a new problem.

1) What steps has the Department of Energy and the National Labs taken, including commercially available open-source intelligence tools, to identify and mitigate the security risks posed by foreign nationals from Countries of Risk working at, or in collaboration, with the DoE National Labs?

.....

Response from Dr. Geraldine Richmond, former Undersecretary for Science and Innovation in the Department of Energy, currently Presidential Chair in Science and Professor of Chemistry at the University of Oregon.

During my time as Undersecretary for Science and Innovation in the Department of Energy, the DOE Laboratories updated and upgraded the Risk Matrix to vet researchers and visitors from foreign contries of concern. This is a very through vetting process. Below is a description of the process (referred to as the Risk Matrix) that the Laboratories use.

Research Security at Department of Energy National Laboratories

DOE National Laboratory Risk Matrix Overview

- For most national labs, the post-doc population – a principal pipeline of R&D talent – is primarily international, which is consistent with the population of graduate students in U.S. universities and the increasing stature of China's R&D programs.
  - This population enables us to attract the most talented researchers to our mission and also to stay engaged with and aware of the full breadth of research frontiers globally.
  - A small fraction of these post-docs are converted to regular staff, some of whom become U.S. citizens.

- Most visits to the laboratories by international colleagues are short, one-time visits through user facilities and guest arrangements, sometimes only through off-site engagement.
- Laboratory research managers partner closely with their colleagues in the DOE Counterintelligence (CI) Field Offices to continuously:
    1. Assess the risk & benefit of individuals from sensitive countries *prior* to employment/granting visitor status (with about 10% of potential employees/visitors rejected when risk exceeds benefit)
    2. Develop and implement risk mitigation plans *during* the laboratory tenure of those colleagues.
    3. Mature approaches to risk-benefit evaluation (e.g., S&T risk matrix) as the landscape continues to evolve, and
    4. Remove individuals from employment if risk-benefit ratio evolves over time.

Description of what the Risk Matrix is:

- The S&T Risk Matrix is the product of a collaborative effort between DOE and the National Laboratories.
- First created in 2019 and updated in 2022, the S&T Risk Matrix was developed to identify and protect emerging areas of research and technology development critical to our economic and international competitiveness, and control who has access to or engages in that research.
- DOE leaders, DOE program managers, and the Chief Research Officers at the national laboratories collaborated in reviewing the current state of technology development and progress in each research field, as well as potential applications, to identify and categorize the risk levels associated with discrete research fields (red, yellow, green) in the matrix and how best to apply the matrix.
- It was designed to supplement, not supplant or supersede, existing controls and protections associated with national security or commerce (e.g., classified information, International Traffic in Arms Regulations (ITAR) or export controls).

Description of how the Risk Matrix works:

- The updated 2022 matrix covers six research and technology areas and quantifies risk and defines necessary controls and mitigation in three categories for each area:
    - **Red/Restricted:** Sensitive emerging technology areas relevant to economic and/or international competitiveness are not to be shared with individuals from countries of risk unless vetted and approved by senior DOE leadership due to the potential for significant harm to the critical national interests of the United States.
    - **Yellow**: Emerging technology areas relevant to economic and/or international competitiveness that have the potential to become Restricted and require enhanced monitoring and controls under certain circumstances before information can be shared with individuals from countries of risk.
    - **Green**: Emerging technology with no particular sensitivity or relevance to economic and/or international competitiveness, such as fundamental scientific research or technologies with a low technology readiness level (TRL).

- Fundamentally, these categories determine the degree to which foreign entities and foreign nationals from countries of risk can access information on the research and technologies covered by the matrix.
- For proposed engagements with entities or foreign nationals from countries of risk, DOE already requires additional reviews and DOE approval before the research even moves forward, much less who has access to it.
    - If the proposed engagement also involves an area of research or technology development identified as Red/Restricted in the S&T Risk Matrix, the engagement is prohibited unless the DOE Site Office manager requests and senior leadership at DOE headquarters at the under secretary level approves an exemption.
    - If the proposed engagement is NOT in an area identified as Red/Restricted in the S&T Risk Matrix, it can proceed based on appropriate DOE review and approval.

Implementation:

- Red/restricted elements of the S&T Risk Matrix is considered Controlled Unclassified Information (CUI); yellow and green topics are not CUI and are broadly disseminated to facilitate awareness, training, and implementation by national laboratory staff.
- DOE plans to update the S&T Risk Matrix annually with the flexibility to edit continuously.
- For the next iteration, DOE intends to consider adding other research topics that are assessed as having potential national or economic security implications that do not otherwise have protections in place, such as classified information or export controls.
- In developing the S&T Risk Matrix, the national lab chief research officers served as ambassadors to the research community to convey the risks and obtain buy-in on potential risk mitigation measures.
- The S&T Risk Matrix only applies to DOE national laboratories and is not currently extended to financial assistance awards that would be accessible to academia.

- **Foreign Nationals Vetting Process**

(Note: While all labs/CI offices manage vetting processes slightly differently, the core functions remain the same)

Laboratory leadership works closely with subject matter experts to include laboratory Counterintelligence, Export Control, and Security officials in order to evaluate the risk posed by foreign nationals who spend any time at the national laboratories. While the specifics of these reviews and databases checked can vary between sites, DOE Orders 142.3B, 475.1, and 486.1A (see order summaries below) provide a framework to vet potential foreign national visitors and longer-term guest scientists. This may include but is not limited to:

1. Counterintelligence briefings and debriefings of foreign nationals' hosts.
2. Checks through US government databases, including those maintained by the FBI and CIA.
3. Specialized enhanced vetting by DOE CI Field Offices
4. Reviews of visitor CVs going back to age 18.

5. Reviews of visitor affiliations including with foreign talent programs.

- **Physical and Cyber Security Measures to Protect Sensitive Research**

  (Note: All DOE sites handle this differently.)
  Each national laboratory develops individual security mitigation plans for foreign national visitors to ensure they are isolated from sensitive research onsite and online. Additionally, a number of laboratory departments and components, including Counterintelligence, Security, Information Technology, Foreign National Access Programs, Classification, and hosts of foreign nationals, work together to ensure these foreign nationals only have access to computer networks and areas of the laboratory needed to conduct their open, unclassified research. The measures taken to protect sensitive research include:
  1. Approved building lists which restrict foreign nationals to buildings and areas where only unclassified work takes place.
  2. Physical security measures such as badge readers, fences, and guards to ensure foreign nationals and others without proper authorization or clearance are unable to access facilities where sensitive work takes place.
  3. Requirements for all foreign nationals to badge-in to all buildings.
  4. Operational Security programs and annual training to remind employees to refrain from classified conversations outside of secure areas.
  5. Information Technology polices which restrict foreign nationals' access to specific portions of unclassified computer networks.
  6. Issuing red badges to foreign nationals and taking other protective steps to help identify their status to other employees and lab security forces.

- **Counterintelligence Infrastructure and Activities at DOE and the National Labs**

  DOE Counter Intelligence (CI) Field Offices collocated at thirteen national laboratories engage in a full complement of defensive CI activities designed to identify and mitigate foreign threats to DOE equities. While not all-inclusive, activities to identify and mitigate threats include:
  - Conducting national security investigations, including but not limited to investigating allegations of espionage, compromise of sensitive information, foreign targeting of DOE and national laboratory employees, foreign cyber intrusions, and international terrorism..
  - Providing counterintelligence analytical support.
  - Providing pre- and post-travel debriefings to laboratory staff authorized by DOE and NNSA to travel to sensitive countries, when travel involves a DOE sensitive technology, or when laboratory staff will be interacting with sensitive country foreign nationals.
  - Vetting visitors and assignees (longer-term guest scientists) to the national labs and the broader DOE complex, especially if they are from a sensitive country, working on sensitive DOE research or technology, or have a prior affiliation with an entity from a sensitive country within the previous 10 years.

- Conducting briefings and debriefings for national lab, DOE, and NNSA personnel who are hosting sensitive country foreign nationals.
- Participating in the Supply Chain Risk Management review processes led by procurement officials, including reviewing and assessing vendors, CRADAs, agreements, procurements, and partnerships.
- Participating in the Laboratory Insider Threat Working Groups .
- Conducting personnel security file reviews .
- Providing Counterintelligence subject matter expertise to lab leadership to support decision-making processes related to foreign engagements, foreign interactions, or lab operations.
- Providing cyber Counterintelligence subject matter expertise to laboratory chief information officers and cyber security representatives.
- Information-sharing with US intelligence community partners.

- **Relevant DOE Orders and Policies**

1. DOE Order 475.1 and Presidential Decision Directive 61 – These orders establish Counterintelligence (CI) Program requirements and responsibilities for the DOE, including the NNSA.
2. DOE Order 142.3B – The order defines DOE's Unclassified Foreign National Access Program (UFNAP). In addition to establishing minimum requirements for foreign nationals to access DOE facilities, the UFNAP program establishes the requirements for documenting and tracking access by foreign nationals to ensure the Department meets its responsibility to protect its assets and deny unauthorized access to sites, information, and technologies.
3. DOE Order 486.1A – The order ensures the continued flow of scientific and technical information consistent with DOE's broad scientific mission, while also ensuring protection of U.S. competitive and national security interests and DOE program objectives; prevents potential conflicts of interest, e.g., financial interests, conflicts of commitment, and outside employment, which may undermine the DOE research enterprise; and limits unauthorized transfers of scientific and technical information. The order compels DOE national laboratories to coordinate with DOE CI Field Offices on matters that may involve foreign government sponsored or affiliated activities with countries of risk.
4. Executive Order 12333 – The order establishes the Executive Branch framework for the country's national intelligence efforts, and for protecting privacy and civil liberties in the conduct of intelligence activities, by defining authorities for Intelligence Community agencies, including DOE.
5. DOE Procedures for Intelligence Activities (US Attorney General signed January 2017) – Procedures intended to enable DOE Intelligence Components to carry out their authorized functions effectively; to provide appropriate assistance to other

elements of the Intelligence Community; and to ensure that DOE intelligence activities and programs are carried out in a manner consistent with the constitutional rights of US persons and other protections provided under applicable law and policy.

6. DOE 45.10 (policy memo) 485.A –Describes DOE requirements for foreign engagements and establishes requirements for CI review of agreements including MOUs, CRADAs, etc.