JANUARY 2021

# A New Institutional Approach to Research Security in the United States

## Defending a Diverse R&D Ecosystem

CSET Policy Brief


AUTHORS

Melissa Flagg

Zachary Arnold

## Table of Contents

## Executive Summary

Most U.S. research and development (R&D) takes place in the private sector. This contributes to three problems that undermine the U.S. government's current research security initiatives.

- The first is a problem of **authority**: the government has little or no authority to regulate research that it does not perform or fund, or to advise researchers on security issues that do not implicate federal laws or funds.

- The second is a problem of **information**: because they are not typically involved in research, government officials (especially in federal law enforcement agencies such as the FBI and Department of Justice) often lack the situational awareness and expertise needed to protect that research.

- The third is a problem of **trust**: many, if not most, American researchers are unfamiliar with law enforcement, skeptical of their motives, and wary of restrictions on scientific openness and collaboration. Because of this, researchers are often unwilling to proactively collaborate with the government, including but not limited to law enforcement, to improve research security.

Today, as China challenges the United States for technological leadership and works to extract technology, data, and know-how from U.S. research institutions, the U.S. government is pursuing an ambitious effort to improve research security throughout the country. This effort seems focused on enforcing conditions for federally funded research related to transparency and conflicts of interest, prosecuting researchers accused of violating these conditions, working with research institutions' leaders and administrators to improve awareness of security threats, and preventing some Chinese nationals from physically entering or participating in research in the United States.

These measures are useful in some cases, but they face the core problems of authority, information and trust outlined above. As a result, any strategy that emphasizes them will inadequately protect the approximately 75 percent of U.S. R&D that is not federally funded.

To better defend U.S. science and innovation from the serious threats it faces, federal officials should rethink their approach—and the role of the government within it. Funding conditions, prosecutions, and the other familiar

tools in the federal arsenal have their value. But to truly protect U.S. R&D, the government needs to empower frontline researchers as true partners. That means investing more in supporting security-informed decision making in business, philanthropy, and academia, and relying less on mandates and punitive tactics. Most of all, it means understanding that although the government has a crucial role to play, it cannot and should not dominate U.S. research security efforts.

To achieve these goals, we propose a new, public-private research security clearinghouse, with leadership from academia, business, philanthropy, and government and a presence in the most active R&D hubs across the United States. Building on promising real-world examples in cybersecurity and other critical domains, this institution would provide researchers on the frontlines, and their funders and managers, with open source information, security-related education and training, decision support resources, and a non-punitive interface with federal partners (when needed). It would conserve limited federal resources by equipping scientists to make security-informed decisions independently, and it would strengthen the government's other research security initiatives by facilitating communication and mutual understanding among researchers, their institutions, and the public sector.

Protecting the United States' R&D advantage demands new infrastructure, built with the needs of researchers and their institutions in mind, and organized to sustain a unique American strength—our dynamic, bottom-up research ecosystem. To ensure that the United States remains the world's science and technology leader for decades to come, federal law enforcement, research funders and oversight agencies should start laying the groundwork for this infrastructure today.

## Context

### Research security is critical

America's adversaries are extracting valuable data, know-how, and intellectual property from U.S. R&D institutions.[1] This is not a new problem. But as China surges ahead in science and technology—fueled, in many cases, by technologies acquired from the United States—the issue of research security is attracting new attention in Washington. In this paper, we define "research security" as preventing foreign actors from acquiring scientific research through means that are illegal or contrary to prevailing norms, such as rewards, deception, coercion, and theft.

The United States' research security challenge emerges from its leading scientific and industrial institutions, which attract interest from around the world, and its relatively open and collaborative research culture, which creates opportunities for exploitation. Other countries have long worked to seize these opportunities.[2] As it develops into a major technological rival and turns further toward authoritarianism, China has attracted particular scrutiny. Experts note that:

> China's technology transfer programs are broad, deeply rooted, and calculated to support the country's development . . . These practices have been in use for decades and provide China early insight and access to foreign technical innovations. . . . [M]any—possibly most—of these transfers are unmonitored and unknown outside China.[3]

Federal authorities are working hard to safeguard the U.S. R&D enterprise from competitors and adversaries, including but not limited to China. Some of their efforts are necessarily secret, but media reports, official statements, and recent prosecutions suggest the current strategy includes:

- Rigorously enforcing conflict-of-interest conditions and disclosure requirements associated with federal research funding, and investigating and prosecuting researchers who violate these conditions;[4]
- Working with leaders and administrators of research institutions to improve awareness of research security threats;[5] and
- Preventing suspected bad actors from participating in U.S. research or accessing U.S. research institutions—for example, by denying them visas,[6] placing new restrictions on their institutions, or targeting

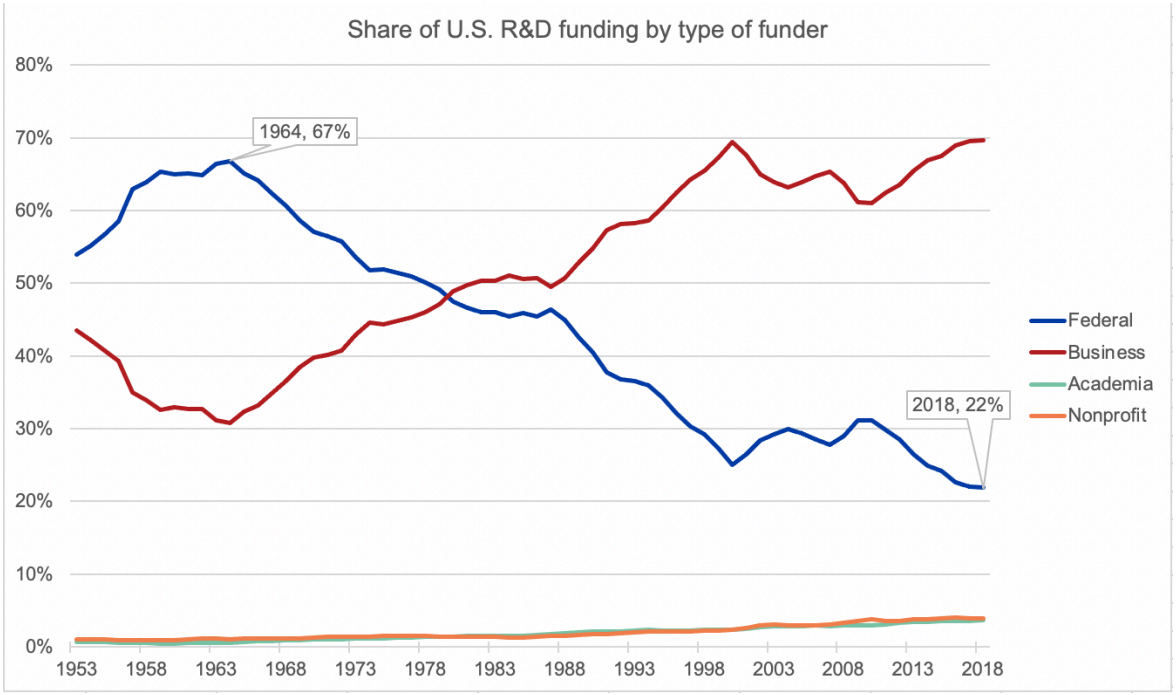
related state-sponsored organizations, such as Confucius Institutes and talent recruitment programs.[7]

## Most research is privately funded and performed

In their speeches on research security, leading federal officials have mixed dramatic warnings with calls for cooperation. "If we are going to maintain our technological leadership, our economic strength, and ultimately our national security in the face of this blitzkrieg," urged then-Attorney General William Barr in a recent speech on China's technology transfer efforts, "we need the public and private sectors to work together and come shoulder-to-shoulder."[8] FBI Director Christopher Wray emphasized that federal agencies like his "can't do it on our own; we need a whole-of-society response, with government and the private sector working together."[9]

Barr and Wray's entreaties point to a basic fact about U.S. R&D: the government is not in command. Now more than ever, the U.S. innovation enterprise is not a top-down system. As shown in Figure 1, according to the most recent data available, less than a quarter of U.S. R&D is federally funded, down from nearly 70 percent in the 1960s. Even in universities, which rely more on public funding than deeper-pocketed corporations, only half of R&D is federally funded.[10] As of last count, the federal share was still falling, meaning federal officials may have even less direct control over the U.S. research enterprise—and the threats it faces—in the years to come.[11]

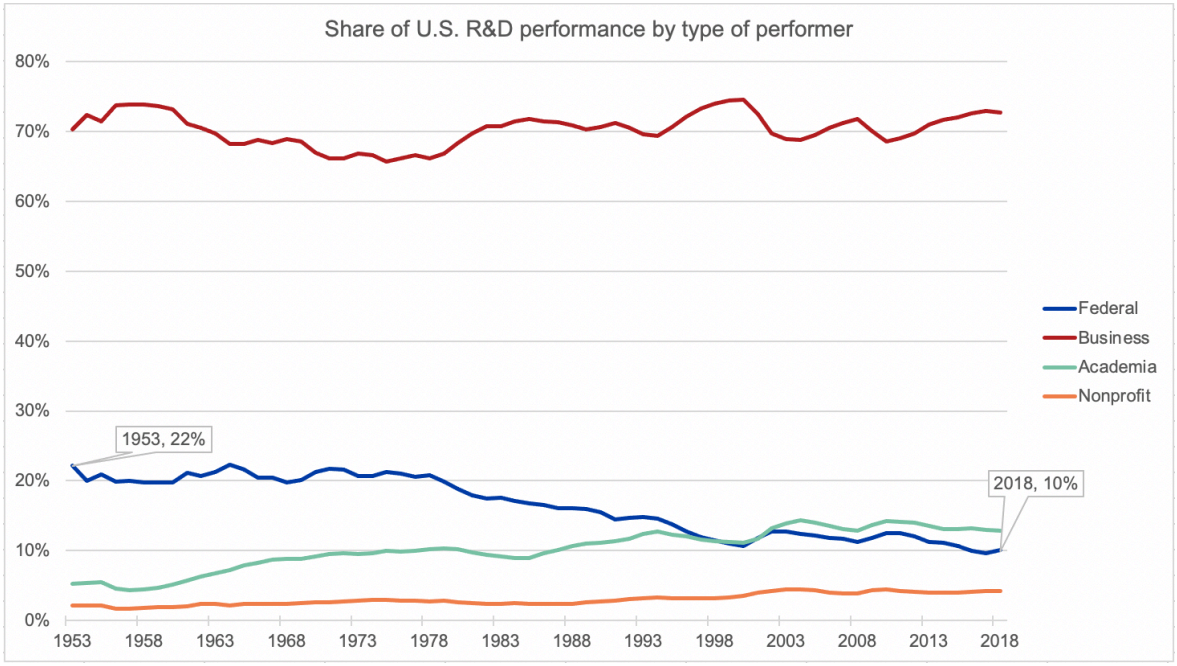
Figure 1. Most U.S. R&D is not federally funded, and the federal share is shrinking




Source: National Patterns of R&D Resources: 2017–18 Data Update, NSF 20-307, Table 6. 2017 and 2018 data are preliminary. "Nonprofit" includes nonprofit organizations outside higher education, as recorded by NSF.

Meanwhile, the federal government's own scientists and engineers perform only 10 percent of total U.S. R&D, as shown in Figure 2.[12] In other words, nearly all U.S. R&D takes place outside the federal government, whether or not the government funds it.

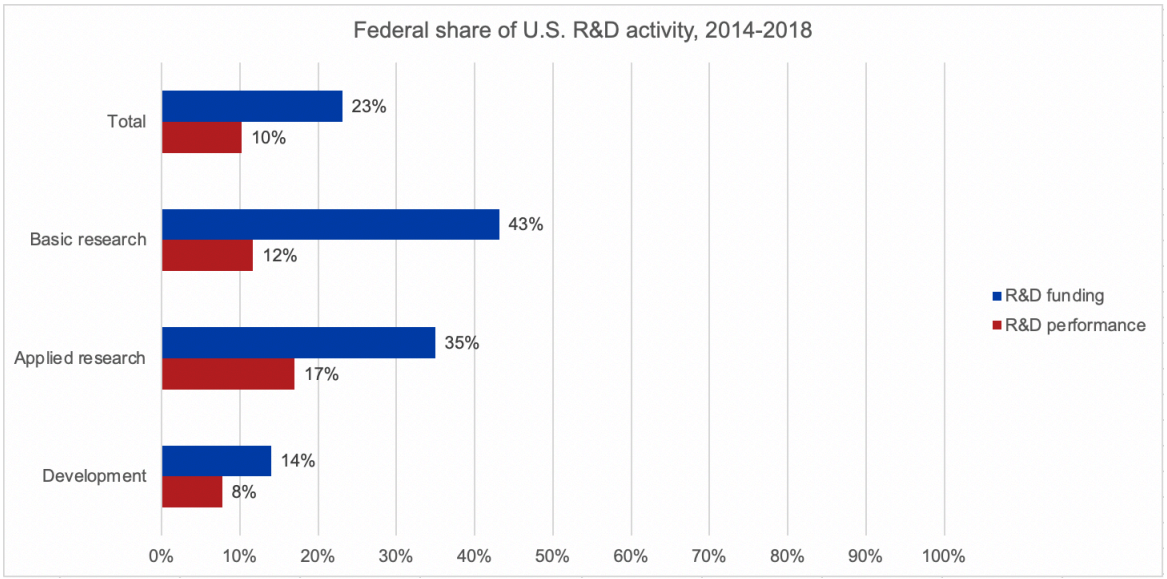
Figure 2. Federal researchers perform a small and declining share of U.S. R&D




Source: National Patterns of R&D Resources: 2017–18 Data Update, NSF 20-307, Table 2. 2017 and 2018 data are preliminary.

The federal government has more sway over crucial basic research, which produces the foundational advances that lead to new products and applications.[13] Still, as Figure 3 shows, most of the United States' basic research is not federally funded, and very little is federally performed. Over the last five years for which data are available, the federal government funded 43 percent of U.S. basic research, compared to 23 percent of all R&D.[14]

Figure 3. The federal presence is limited across all phases of R&D




Source: National Patterns of R&D Resources: 2017–18 Data Update, NSF 20-307, Tables 2-9. Calculations include data from years 2014-2018, inclusive. Funding data are in constant 2012 dollars. 2017 and 2018 data are preliminary.

If the federal government significantly boosts its R&D budget, as many lawmakers are urging, the public share of R&D funding and performance could rise.[15] But it would take a truly massive, decades-long reversal in policy to alter the basic trends presented here. For the foreseeable future, most of the U.S. research enterprise will remain outside the government's direct control.

## Challenges

The public sector's limited and shrinking role in U.S. R&D contributes to three problems for the federal government: a problem of authority, a problem of information, and a problem of trust. These problems are undermining the government's current research security efforts, underscoring the urgent need for new, complementary strategies that engage non-federal partners and resources.

### Authority

Federal officials have limited authority; they cannot act unless federal law authorizes them to act. In the research security context, they have two typical jurisdictional "hooks."

First, they can rely on laws that directly regulate foreign countries' and foreign nationals' interactions with the United States. For example, the interagency Committee on Foreign Investment in the United States (CFIUS) can block corporate mergers and acquisitions that pose national security risks,[16] the Foreign Agents Registration Act requires disclosure of certain foreign agents' activities,[17] and immigration and export control laws restrict some foreigners' access to U.S. R&D.[18]

In some cases, such tools can be used to address research security issues, but they do not provide anything close to comprehensive federal jurisdiction.[19] Some laws exempt broad categories of R&D; most famously, export controls have long exempted "fundamental research."[20] Other laws relevant to research security empower only a limited group within the government to act,[21] prevent federal officials from sharing information with others,[22] or impose significant procedural or evidentiary burdens.[23] There are usually good reasons for these caveats.[24] Nonetheless, they make it less likely that any particular federal official will be able to act on research security threats as they emerge. The threats may not meet that official's narrow jurisdictional criteria, or the official may not have the legal tools to adequately respond.[25]

Second, the government can attach strings to federal money, giving it much more flexibility to enforce research security—as long as the research is federally funded. For example, Charles Lieber, the recently arrested chair of Harvard University's chemistry department, allegedly violated disclosure terms in his federal grants by joining China's Thousand Talents recruitment program without informing his National Institutes of Health (NIH) and Department of Defense funders.[26]

All of the major federal funding agencies require grantees to disclose conflicts of interest, including conflicts involving foreign entities, and restrict grantee activities that may pose research security threats. These grant conditions can extend broader and deeper than research security laws; joining Thousand Talents may not be illegal in itself, but not disclosing it to the NIH (for example) could mean federal charges.[27] Not coincidentally, researcher prosecutions under the Department of Justice's "China Initiative" routinely involve violations of federal grant conditions.[28]

Although these conditions give federal officials authority and flexibility, they extend only as far as federal funding does. Today, most R&D in the United States is privately funded, and relatively few researchers rely on federal resources, especially outside of academia. Many receive no federal funding at all. For others—in particular, researchers who are already well-established, or who work on more commercializable technologies—federal grants are helpful, but not necessary. If conditions on federal grants become more burdensome, these researchers could simply opt for private money, frustrating research security efforts and reducing the government's access to cutting-edge science, as discussed below.[29]

In sum, federal officials have limited authority to act on research security threats. The most relevant federal laws are far from comprehensive. Funding conditions give some additional coverage, but leave wide swaths of the U.S. research enterprise untouched. Any research security strategy that relies on federal jurisdiction will miss a great deal.

## Information

The U.S. R&D enterprise encompasses millions of scientists and engineers, hundreds of research universities, and uncounted corporate and nonprofit labs.[30] Monitoring this vast and dynamic ecosystem, much less adequately defending it, would challenge even the best-equipped federal agencies.[31] The specialized nature of cutting-edge research is another obstacle. In many disciplines, understanding which research results and technologies are valuable targets, or communicating productively with rank-and-file researchers, can require an advanced degree and lab experience. Relatively few federal employees have these, especially within law enforcement agencies such as the FBI and Department of Justice.[32]

Again, the federal government's limited role in U.S. research adds to these informational challenges. Through the grant application process and ongoing interactions with their grantees, federal agencies gather rich data from the

researchers they fund. As federal grants become less common, funding agencies build relationships with and gather information from a shrinking share of researchers. Meanwhile, as the government itself performs relatively less research over time, it loses access to scientific contacts and information networks, and fewer of its personnel have the training and practical experience needed to stay abreast of cutting-edge scientific research.

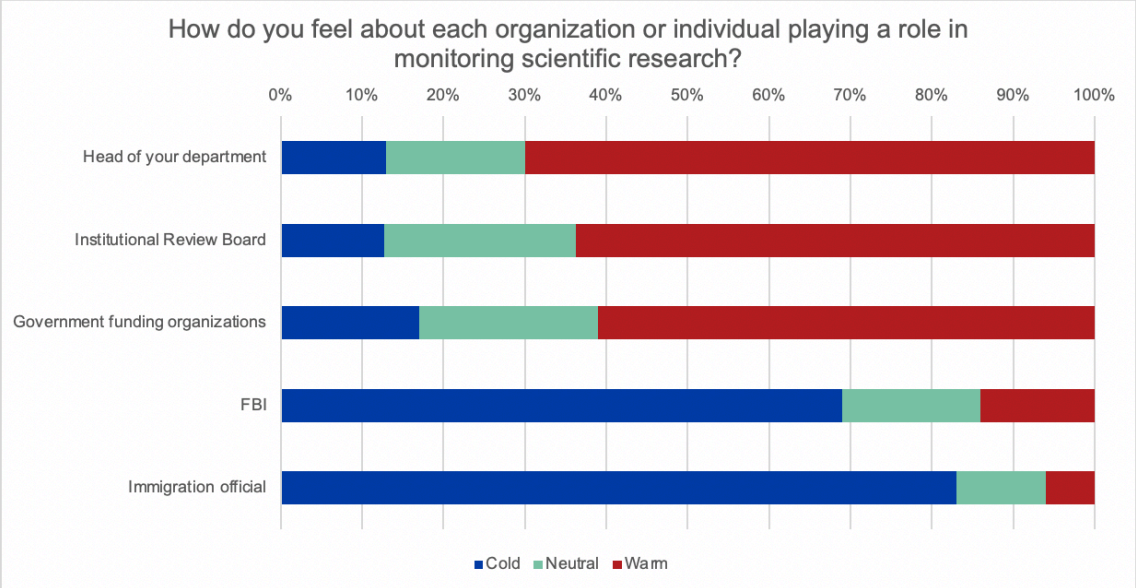
Collectively, these trends leave the federal government less informed about current research—and the threats it faces.

## Trust

A "whole-of-society" response to the research security threat requires close and proactive cooperation from the research community. But cooperation requires trust, and in many cases, U.S. researchers are wary of government interventions into their work.

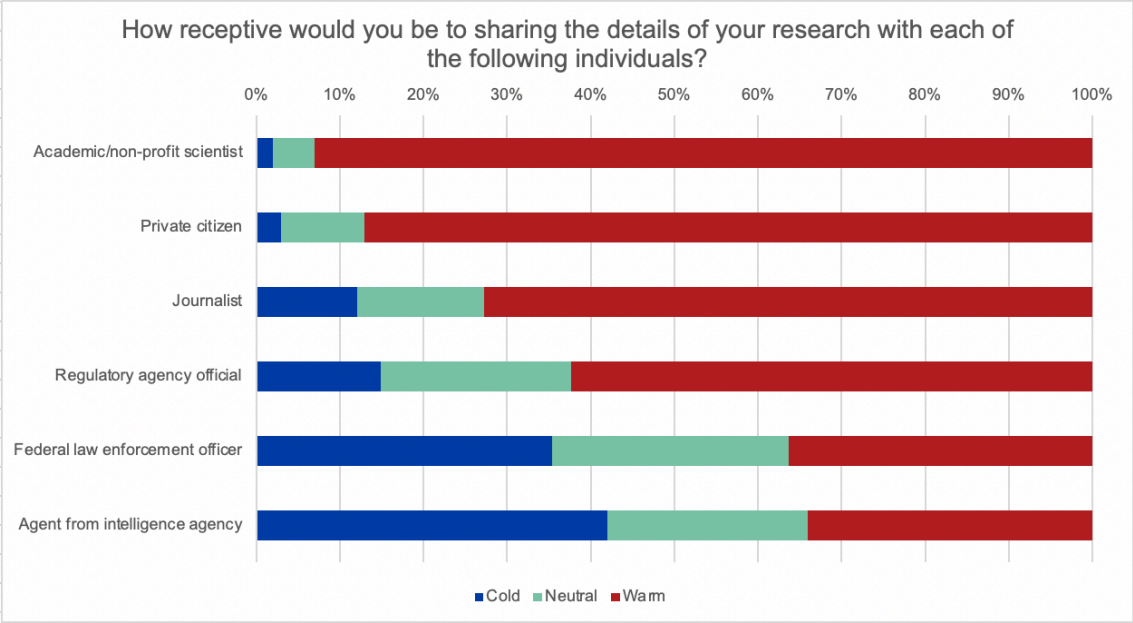
One study, conducted by the Federation of American Scientists (FAS) and the FBI in 2009, concluded that "scientists are suspicious of the FBI and feel that they do not work well with the scientific community." More than three quarters of the scientists polled agreed that law enforcement "[did] not understand their work." As shown in Figures 4 and 5, respondents overwhelmingly felt that federal law enforcement should have no role in monitoring scientific research, and most were reluctant to share information with federal officials.[33]

Figure 4. Researchers believe federal law enforcement should not be involved in monitoring research




Source: FAS/FBI survey of 1,332 scientists (conducted 2009).

Figure 5. Researchers are reluctant to share information with federal officials




Source: FAS/FBI survey of 1,332 scientists (conducted 2009)

Of course, researchers can have their own misconceptions. Law enforcement officials worry that scientists and their institutions are naive, uninformed, or simply apathetic about research security, and too quick to dismiss federal efforts to protect them and their work.[34] These concerns are sometimes justified. Some researchers have yet to recognize the reality of twenty-first century science and technology; today, "dual use" is ubiquitous, repressive governments center R&D in their strategies for dominance, and at least one major research power—China—systematically exploits scientific norms of neutrality, transparency, and open collaboration for its own geopolitical purposes.[35]

However, misconceptions cannot entirely explain researchers' mistrust of the federal government. To some extent, this mistrust may be unavoidable. The open-science norms that enable U.S. technological leadership, and scientific progress more generally, are often in tension with research security goals. Researchers cherish these ideals and are understandably wary of perceived interference.[36] In some cases, they may have broader concerns about governments' inevitable interest in using science and technology for their own geopolitical ends. The U.S. free-enterprise system is also a factor. Most U.S. R&D takes place within private companies that are focused on the bottom line rather than public priorities, are generally skeptical of regulation, and may have financial motives to doubt warnings about research security.[37]

In other ways, the federal government has not helped its own case. Very few federal counterintelligence agents have an understanding of the research environment—and too few understand the foundations of openness and research integrity that are scientists' and engineers' unspoken "rules of the road."[38] To be sure, law enforcement is only one part of the federal government. But this nuance is often lost on scientists not well versed in the government's ins and outs. And in fairness to these scientists, research funders and law enforcers do communicate and collaborate regularly—for example, as part of routine interagency processes, or in the course of investigations related to federal science.[39] For these reasons, law enforcement and its actions may color researchers' perceptions of the federal government as a whole.[40]

Finally, the government's shrinking presence in R&D may deepen the gap in trust. The FAS survey results indicate that researchers trust federal funding agencies much more than they trust law enforcement.[41] When close to 70 percent of research was federally funded, the federal government was the primary driver of research topics and funding for most U.S. researchers. There were also fewer scientists and engineers, and a smaller set of funding agencies. As a result, scientific communities were more deeply intertwined with the federal government, including on a personal level.

But as the government becomes a smaller input to the U.S. R&D ecosystem, and as that ecosystem continues to grow, a smaller share of researchers build relationships with federal employees. Meanwhile, relatively fewer government agencies and employees develop an understanding of the scope and breadth of U.S. research communities, which could make researchers worry that federal officials may misinterpret normal activities as security threats. More broadly, tighter federal science budgets—and proposals to cut them further, a fixture in recent years—can set a tone of disregard, even contempt, for the scientific community.[42] Direct evidence of these dynamics is hard to come by, but at a minimum, the federal government probably has not built trust by contributing proportionately less to U.S. research over the years.

## One path forward

The federal government lacks the authority, information, and trust it would need to secure U.S. research on its own. The basic challenge is structural: the U.S. research enterprise is just too big, too distributed, too complex, and too exposed across too many sectors for a top-down, federally controlled approach to the research security challenge. Even if the resources and political will existed to allow it, imposing this approach would destroy research as the United States knows it, eroding the values of collaboration and free inquiry that fuel its scientific and technological advantage.

At the same time, we cannot expect U.S. private-sector research organizations to solve the problem themselves. Even the best-resourced corporations and universities cannot always deter sophisticated, state-sponsored research security threats.[43] In some cases, private-sector institutions and researchers may not be aware enough of security threats to properly defend themselves in the first place.[44] And even if individual institutions could perfectly defend their intellectual property, they might withhold threat intelligence from their competitors, or decide to transfer technology in exchange for short-term profits, without properly understanding the broader costs of doing so to themselves and others.[45]

To make better progress, the federal government should help build or encourage private investment in new institutional infrastructure for research security, and incentivize non-federal stakeholders to do the same. We envision a new institution, empowered by the government—but not run by the government—to study and act on all kinds of relevant developments, not just those that implicate federal laws. The institution would have resources that will allow it to elicit, process and share open source analysis from all corners of the global research enterprise,[46] including experienced technical and development personnel, access to data and analytic tools, and strong relationships with industry, academia, philanthropy, and other private research institutions. And to earn researchers' trust and active cooperation, it would offer them accessible, non-punitive pathways to share concerns and receive advice—and it would be meaningfully independent from the government.

To meet these urgent needs, the federal government should convene and provide seed funding for an independent research security clearinghouse, with leadership from academia, philanthropy, business and government. This organization would use open source data to analyze and document the shifting technology landscape, generate context-specific, data-driven

assessments and best practices, and develop frameworks that help researchers apply these insights in their day-to-day activities, such as hiring, traveling, and collaborating with others. The government would serve as a partner, providing financial and technical support where appropriate—but allow the nominal institution or consortium to drive the business model through consultations with the interested parties.

By participating in this new public-private institution, researchers and their organizations would be equipped to collaborate, sell, and attract talent around the world without putting their intellectual property at risk. For private industry, this would be a unique source of competitive intelligence; for universities, a safeguard in recruiting the world's best and brightest; and for all participants, a means of heading off the legal trouble, regulatory scrutiny, and reputational damage that can result when research security is compromised. Perhaps most importantly, for the very many rank-and-file researchers who want to "do the right thing," it would offer help without the threat of misunderstanding, or worse.

Although some forums already exist to promote public-private collaboration around research security issues, and others have been proposed, none comes close to fulfilling the role and providing the resources we envision. For example, the National Defense Authorization Act for fiscal year 2020 included a new Science, Technology and Security Roundtable, with representatives from government, academia, and industry, to share information related to research security and explore new approaches to the issue.[47] While these sorts of forums can help set the research security agenda, build trust, and develop best practices, they are not designed to provide the specific, actionable information and support that frontline researchers need, and they lack the analytic resources and broad research community buy-in that it will take to make a real dent in the research security challenge.

To our knowledge, the more extensive model we advocate has not been used for research security yet, but it has supported progress in other domains. In particular, the U.S. cybersecurity infrastructure relies heavily on public-private institutions and industry self-regulatory organizations. As with research security, cybersecurity involves defending a massive, diverse attack surface that largely exists in the private sector. To confront this similar challenge, in 2002, federal and private-sector partners established the National Cyber-Forensics and Training Alliance (NCFTA), "a nonprofit partnership between private industry, government, and academia for the sole purpose of providing a neutral, trusted environment that enables two-way collaboration and cooperation to identify, mitigate, and disrupt cyber crime."[48] Working from

unclassified office space near Carnegie Mellon University, NCFTA's team, which includes private-sector analysts, federal investigators, and cybersecurity scholars, has prevented billions of dollars in losses and referred thousands of cases to law enforcement.[49]

Many critical sectors also operate their own Information Security and Analysis Centers (ISACs) and Information Security and Analysis Organizations (ISAOs), secure forums for private companies to share cyber threat intelligence with each other, often in collaboration with federal agencies.[50] At their best, these organizations can become valuable assets. According to one recent analysis, "Many ISACs are well resourced, come with membership fees and have infrastructure and full-fledged security operations centers for monitoring threats on a global scale. . . . Information being shared in [one successful ISAO] includes [everything] from rogue email and IP addresses to best practices and equipment vulnerabilities."[51]

Finally, outside the cyber domain, industries from finance to nuclear energy have built self-regulatory organizations to promote best practices, discipline laggards, and interface with relevant authorities as needed.[52] Again, many of these organizations have meaningfully improved security for their members and host industries.[53]

Building a similar institution would go a long way toward protecting U.S. research from the security threats it faces. To that end, we offer the following initial recommendations:

- The Office of Science and Technology Policy (OSTP), or a designated agency such as the National Science Foundation (NSF) and/or the National Institute of Standards and Technology (NIST), in cooperation with scientific, academic, and industry organizations such as the National Academies, American Association for the Advancement of Science, Association of American Universities, Institute of Electrical and Electronics Engineers, Business Roundtable, and Council on Competitiveness, should convene regional (possibly virtual) listening sessions with the R&D community. Outreach would target large private funders of research in industry and philanthropy as well as large producers of R&D in industry and academia, but also ensure participation from startups, incubators and accelerators, private labs, and smaller research universities. These sessions would allow the federal government to discuss its perspective and concerns, and for the participants to provide insights on their own perspectives, needs, and desired incentives for participating in security efforts.

- In parallel, OSTP, or a designated agency such as NSF and/or NIST, should commission a study to provide options for business models and cost structures for the new institution. As part of this effort, the study should explore products and services that could eventually be provided on a subscription basis. These might include technology landscape assessments regularly updated for priority technology areas, as well as running assessments of global scientific research, intellectual property production, and market activity.

- Finally, the United States should establish an advisory group with representatives of the largest non-federal sources of R&D funding—industry, academic endowments, and philanthropic donors—to begin a candid dialogue on scientific norms and incentives in a multipolar era. This group would convene annually to discuss steps toward reconciling scientific openness, profitability, economic development, and the very real security concerns of a multipolar world where technology may often be the determinant of power, and competitor nations may distort or exploit longstanding norms for their own gain.

With their broad perspective and national security mission, federal authorities are well-positioned to help build new infrastructure to meet the research security challenge, and their unique legal and financial resources will be an important aspect in establishing a credible institution. But the federal government must begin to shift perspective. In a research environment where it is not the sole or primary driving force, the government must be able to act as a trusted partner, not a commander.

U.S. R&D has been a global model for over 70 years because it is diverse, dynamic, and very often bottom-up, sustained not only by the government but by an amazing multiplicity of corporate, academic, philanthropic, and nonprofit institutions. This is both a great strength and a large challenge in the multipolar era. The approaches that sustained U.S. R&D enterprise for the last 70 years are likely not the exact same approaches that will provide a foundation for leadership in the decades to come. Those charged to protect this critical asset must embrace its diversity and its dynamism.

## Acknowledgments

Thanks to Danny Hague, Paul Harris, Shalin Jyotishi, Ngor Luong, Igor Mikolic-Torreira, Dahlia Peterson, Anna Puglisi, Emily Weinstein, and Remco Zwetsloot for thoughtful comments and Melissa Deng for production assistance. The authors are solely responsible for the views expressed in this piece and for any errors.



Document Identifier: doi: 10.51593/20200051

## Endnotes

[1] See generally William Hannas and Huey-Meei Chang, "China's Access to Foreign AI Technology: An Assessment" (Center for Security and Emerging Technology, September 2019), https://cset.georgetown.edu/wp-content/uploads/CSET_China_Access_To_Foreign_AI_Technology.pdf; National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace* (Washington, DC: Director of National Intelligence, 2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[2] See, e.g., National Counterintelligence and Security Center, *Foreign Economic Espionage*; Hannas and Chang, "China's Access to Foreign AI," 3-4; Milton J. Socolar, "Economic Espionage: The Threat to U.S. Industry," Testimony to the Subcommittee on Economic and Commercial Law, Committee on the Judiciary at the House of Representatives, 102nd Congress, April 29, 1992, https://www.gao.gov/assets/110/104477.pdf.

[3] Hannas and Chang, "China's Access to Foreign AI," iii.

[4] See, e.g., Jeffrey Mervis, "NSF's Handful of Foreign Influence Cases May Be Due to How It Investigates Them," *Science*, July 14, 2020, https://www.sciencemag.org/news/2020/07/nsf-s-handful-foreign-influence-cases-may-be-due-how-it-investigates-them-0; U.S. Department of Justice, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," January 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related; U.S. Department of Justice, "Former Emory University Professor and Chinese 'Thousand Talents' Participant Convicted and Sentenced for Filing a False Tax Return," May 11, 2020, https://www.justice.gov/opa/pr/former-emory-university-professor-and-chinese-thousand-talents-participant-convicted-and. The government has investigated institutions as well as individuals. See, e.g., U.S. Department of Education, "U.S. Department of Education Launches Investigation into Foreign Gifts Reporting at Ivy League Universities," February 12, 2020, https://www.ed.gov/news/press-releases/test-0.

[5] Christopher Wray, "Responding Effectively to the Chinese Economic Espionage Threat," February 6, 2020, Department of Justice China Initiative Conference (Center for Strategic and International Studies), https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat; Nidhi Subbaraman, "Universities Are Forging Ties with the FBI as US Cracks Down on Foreign Influence," *Nature*, March 12, 2020, https://www.nature.com/articles/d41586-020-00646-9.

[6] President, Proclamation, "Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China," *Federal Register* 85 (June 4, 2020): 34353-34355, https://www.whitehouse.gov/presidential-actions/proclamation-suspension-entry-nonimmigrants-certain-students-researchers-peoples-republic-china/. However, visa restrictions can be circumvented. See "Global Engagement: Rethinking Risk in the Research Enterprise" (Hoover Institution, July 30, 2020), 13, 23, https://www.hoover.org/global-engagement-rethinking-risk-research-enterprise.

[7] See, e.g., Cheryl Arcibal, "US Slaps Sanctions on 33 Chinese Companies and Institutions, Dialling up the Tension Amid the Lowest Point in US-China Relations," *South China Morning Post*, May 23, 2020, https://www.scmp.com/business/companies/article/3085788/us-slaps-sanctions-33-chinese-companies-and-institutions; Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," July 7, 2020, Hudson Institute, https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states; U.S. Department of State, "'Confucius Institute U.S. Center' Designation as a Foreign Mission," August 13, 2020, https://www.state.gov/confucius-institute-u-s-center-designation-as-a-foreign-mission/. See also Bureau of Industry and Security, "Deemed Exports," U.S. Department of Commerce, https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.

[8] William Barr, "Attorney General William Barr's Keynote Address: China Initiative Conference," February 6, 2020, Department of Justice China Initiative Conference (Center for Strategic and International Studies), https://www.csis.org/analysis/attorney-general-william-barrs-keynote-address-china-initiative-conference.

[9] Wray, "Responding Effectively to the Chinese Economic Espionage Threat."

[10] Beethika Khan, Carol Robbins, and Abigail Okrent, "The State of U.S. Science and Engineering 2020: U.S. R&D Performance and Funding," National Center for Science and Engineering Statistics, January 15, 2020, https://ncses.nsf.gov/pubs/nsb20201/u-s-r-d-performance-and-funding.

[11] Khan, Robbins, and Okrent, "The State of U.S. Science and Engineering"; John F. Sargent Jr., "U.S. Research and Development Funding and Performance: Fact Sheet," Congressional Research Service, January 24, 2020, https://fas.org/sgp/crs/misc/R44307.pdf, 2. This analysis omits spending on R&D plant, which includes "R&D facilities and fixed equipment, such as reactors, wind tunnels, and particle accelerators." U.S. National Science Foundation, "Federal Funds Survey Glossary," https://www.nsf.gov/statistics/fedfunds/glossary/def.htm. This is a relatively small category. In FY 2018, federal obligations for R&D plant totaled $3.9 billion, compared to $133.3 billion for R&D. Christopher Pece, "Federal R&D Obligations Increase 8.8% in FY 2018; Preliminary FY 2019 R&D Obligations Increase 9.3% Over FY 2018," U.S. National Science Foundation, January 30, 2020, https://www.nsf.gov/statistics/2020/nsf20308/, Table 1.

[12] Khan, Robbins, and Okrent, "The State of U.S. Science and Engineering."

[13] See, e.g., U.S. National Science Foundation, "America's Share Decreasing as Global Science and Engineering Grows," January 15, 2020, https://www.nsf.gov/nsb/news/news_summ.jsp?cntn_id=299790 ("'Federal support of basic research drives innovation. Only the Federal government can make a strategic, long-term commitment to creating new knowledge that cannot be anticipated to lead to new or improved technologies, goods, or services,' said Julia Phillips, Chair of NSB's Science and

Engineering Policy Committee. 'Basic research is the "seed corn" of our U.S. S&E enterprise, a global competitive advantage, and the starting point for much of our GDP growth since World War II.'").

[14] Again, this analysis omits the relatively small amount of spending on R&D plant. See note 11 above.

[15] Jeffrey Mervis, "U.S. Lawmakers Unveil Bold $100 Billion Plan to Remake NSF," *Science*, May 26, 2020, https://www.sciencemag.org/news/2020/05/us-lawmakers-unveil-bold-100-billion-plan-remake-nsf.

[16] James K. Jackson, "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service, February 14, 2020, https://fas.org/sgp/crs/natsec/RL33388.pdf.

[17] "The Foreign Agents Registration Act ('FARA'): A Guide for the Perplexed," Covington & Burling LLP, July 26, 2019, https://www.cov.com/-/media/files/corporate/publications/2018/01/the_foreign_agents_registration_act_fara_a_guide_for_the_perplexed.pdf.

[18] See, e.g., Bureau of Industry and Security, "Deemed Exports."

[19] See, e.g., Hannas and Chang, "China's Access to Foreign AI," 3-4 ("[M]ost of the features comprising [China's technology transfer] program are—in terms of vectors alone—not necessarily illegal, which renders the question of policy response all the more difficult."); U.S. Department of Justice, "The China Initiative: Year-in-Review (2019-20)," November 16, 2020, https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20 ("While membership in these talent programs is not per se illegal, and the research itself may not always be protected as a trade secret, we know the PRC uses these plans, such as the well-known Thousand Talents Program, as a vehicle to recruit individuals with access to U.S. government-funded research to work in the interest of the Chinese Communist Party" (quoting Adam S. Hickey, Deputy Assistant Attorney General, National Security Division)).

[20] See U.S. National Science Foundation, "Statement of the National Science Board on Security and Science," October 24, 2018, https://www.nsf.gov/news/news_summ.jsp?cntn_id=297039.

[21] See, e.g., "Executive Order 12333 of December 4, 1981," *Federal Register* 85 (December 4, 1981): 59941, https://www.archives.gov/federal-register/codification/executive-order/12333.html (restricting specified U.S. intelligence agencies from collecting information on U.S. citizens and permanent residents).

[22] See generally Robert K. Knake, "Sharing Classified Cyber Threat Information With the Private Sector" (Council on Foreign Relations, May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector ("[D]isseminating collected information outside the intelligence community remains time-consuming and difficult. Information either needs to be declassified to be shared or can only be shared in in-person briefings with the small number of individuals at private companies

who have clearances."); JASON, "Fundamental Research Security" (The MITRE Corporation, December 2019), 37, https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

[23] See, e.g., Asha Rangappa, "It Ain't Easy Getting a FISA Warrant: I Was an FBI Agent and Should Know," Just Security, March 6, 2017, https://www.justsecurity.org/38422/aint-easy-fisa-warrant-fbi-agent/ (describing the procedural hurdles federal agencies must clear in order to conduct domestic surveillance).

[24] See, e.g., JASON, "Fundamental Research Security," 4 ("[T]he 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.").

[25] See Christian Berthelsen, "Prosecutors Say They're Spies, But Charges Tell a Different Story," *BloombergQuint*, October 22, 2020, https://www.bloombergquint.com/businessweek/u-s-calls-chinese-visa-offenders-spies-without-showing-evidence ("Across the country in recent months, prosecutors have begun telling the public that they're cracking down on nefarious behavior by visiting scientists from China, sometimes labeling them "spies" or implying their cases involved threats to national security. . . [But a] review of court filings and transcripts of hearings shows the charges and allegations are far less serious, frequently involving misstatements surrounding a visa application — a violation often punished with less than a year in prison."). This problem is not limited to research security. See, e.g., "Here's How You Get Companies to Talk to Law Enforcement," *TAG Cyber Law Journal*, May 2019, https://www.cyberinsecuritynews.com/ncfta ("We exist to enable industry to have a seat at the table and have a direct voice to the government or law enforcement in order to identify the things that are impacting them the most. Otherwise, from my background in law enforcement, it's very reactive. A victim would call a local office and report a crime. Unfortunately, whether that agency has the ability to open a case on that specific incident depends on their office resources and capabilities and also on the local prosecutor's office. If that incident is highly impactful to a particular victim or company, but it can't be investigated because it doesn't meet those thresholds, where does that go? What we strive to do is have those things reported through us so that we can connect that with another victim, and another victim, and another victim, and then link the seemingly one-off incidents and make it actionable for law enforcement.").

[26] U.S. Department of Justice, "Harvard University Professor Indicted on False Statement Charges," June 9, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-indicted-false-statement-charges.

[27] To make the analogy between Lieber's prosecution and Al Capone's clearer, he now faces additional tax-related charges. See U.S. Department of Justice, "Harvard University Professor Charged with Tax Offenses," July 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-charged-tax-offenses.

[28] See Jack P. DiCanio et al, "DOJ's 'China Initiative' Uses Scheme-to-Defraud Charges for Nondisclosure of Ties to China," Skadden, Arps, Slate, Meagher & Flom LLP, April 2, 2020,

https://www.skadden.com/insights/publications/2020/04/dojs-china-initiative. Visa fraud is another common predicate. See, e.g., U.S. Department of Justice, "Chinese Government Employee Charged in Manhattan Federal Court with Participating in Conspiracy to Fraudulently Obtain U.S. Visas," September 16, 2019, https://www.justice.gov/opa/pr/chinese-government-employee-charged-manhattan-federal-court-participating-conspiracy.

[29] See, e.g., "Interview Between John Krige and Research Scientist 1," Georgia Institute of Technology, November 2, 2012, 11-12, https://smartech.gatech.edu/bitstream/handle/1853/56410/interview_jk_with_rs1.pdf.

[30] See generally John F. Sargent Jr., "The U.S. Science and Engineering Workforce: Recent, Current, and Projected Employment, Wages, and Unemployment," Congressional Research Service, November 2, 2017, https://fas.org/sgp/crs/misc/R43061.pdf; "2018 Update: Facts & Figures," The Carnegie Classification of Institutions of Higher Education, May 24, 2019, https://carnegieclassifications.iu.edu/downloads/CCIHE2018-FactsFigures.pdf.

[31] The federal government's limited open source intelligence capabilities compound this problem. See Tarun Chhabra et al, "Open-Source Intelligence for S&T Analysis" (Center for Security and Emerging Technology, September 2020), https://cset.georgetown.edu/wp-content/uploads/CSET-Policy-Recommendation-OSINT-One-Pagers.pdf.

[32] See JASON, "Fundamental Research Security," 37 ("[T]he IC and law enforcement agencies lack an understanding of how academic research labs operate, and the advising and mentoring relationships that exist between faculty members and the range of researchers who work with them.").

[33] Nathaniel Hafer et al, "How Scientists View Law Enforcement: New Survey of Researchers Tells Us How to Help the Communities Communicate," *Science Progress*, 2-3, February 2009, https://www.scienceprogress.org/wp-content/uploads/2009/02/how_scientists_view_law_enforcement.pdf. More recent survey data are not available, but other evidence, from scientist-led protests to employee activism within leading U.S. tech companies, suggests that today's research community might have even less faith in the federal government than in 2009. See, e.g., Chris Mooney, "Historians Say the March for Science is 'Pretty Unprecedented,'" *The Washington Post*, April 22, 2017, https://www.washingtonpost.com/news/energy-environment/wp/2017/04/22/historians-say-the-march-for-science-is-pretty-unprecedented/; Billy Mitchell, "Google's Departure from Project Maven Was a 'Little Bit of a Canary in a Coal Mine,'" *Fedscoop*, November 5, 2019, https://www.fedscoop.com/google-project-maven-canary-coal-mine/; Rebecca Heilweil, "Big Tech Companies Back Away from Selling Facial Recognition to Police. That's Progress," *Vox*, June 11, 2020, https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police.

[34] See, e.g., Barr, "Attorney General William Barr's Keynote Address," ("[M]any in the private sector have too often been willing to countenance China's hardball tactics. . . . To our private-sector friends, I would say that appeasing the PRC may come with short-term benefits, but I urge you to question the longstanding assumption that promises of market access are

worth the steep costs."); Elizabeth Redden, "The Chinese Student Threat?", *Inside Higher Ed*, February 15, 2018, https://www.insidehighered.com/news/2018/02/15/fbi-director-testifies-chinese-students-and-intelligence-threats ("[T]he use of nontraditional collectors, especially in the academic setting . . . . It's not just in major cities. It's in small ones as well. It's across basically every discipline. And I think the level of naïveté on the part of the academic sector about this creates its own issues."); see also JASON, "Fundamental Research Security," 2 ("[A]cademic 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.").

[35] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (Routledge, 2013); Hannas and Chang, "China's Access to Foreign AI."

[36] See generally David A. Hollinger, "Free Enterprise and Free Inquiry: The Emergence of Laissez-Faire Communitarianism in the Ideology of Science in the United States," *New Literary History* 21, no. 4 (1990): 897-919, http://www.jstor.com/stable/469191; Janet Atkinson-Grosjean and Cory Fairley, "Moral Economies in Science: From Ideal to Pragmatic," *Minerva* 47 (2009): 147-170, https://link.springer.com/article/10.1007/s11024-009-9121-7.

[37] See, e.g., "23rd Annual Global CEO Survey: Navigating the Rising Tide of Uncertainty," PwC, 2020, 13, https://www.pwc.com/gx/en/ceo-survey/2020/reports/pwc-23rd-global-ceo-survey.pdf (citing overregulation as a leading concern); Edward Tse, "Why China is Too Important a Market for Foreign Companies to Exit, Especially as Chinese Innovation Takes Off," *South China Morning Post*, November 19, 2018, https://www.scmp.com/comment/insight-opinion/united-states/article/2173602/why-china-too-important-market-foreign.

[38] See JASON, "Fundamental Research Security," 37 ("[T]he IC and law enforcement agencies lack an understanding of how academic research labs operate, and the advising and mentoring relationships that exist between faculty members and the range of researchers who work with them.").

[39] See, e.g., U.S. Government Accountability Office, *National Biodefense Strategy: Additional Efforts Would Enhance Likelihood of Effective Implementation* (Washington, DC: 2018), 12, https://www.gao.gov/assets/710/704698.pdf; U.S. Department of Justice, "Former Virginia Tech Professor Sentenced for Grant Fraud, False Statements, Obstruction," September 9, 2019, https://www.justice.gov/usao-wdva/pr/former-virginia-tech-professor-sentenced-grant-fraud-false-statements-obstruction ("I am proud of the work of the men and women with the National Science Foundation (NSF), Department of Energy, and Federal Bureau of Investigation for conducting a thorough investigation." [quoting First Assistant United States Attorney Daniel P. Bubar]). Law enforcement has also taken a high profile in the federal government's recent research security push. See, e.g., Betsy Woodruff Swan, "Inside DOJ's Nationwide Effort to Take on China," *Politico*, April 7, 2020, https://www.politico.com/news/2020/04/07/justice-department-china-espionage-169653.

[40] The same is probably true of the president and other high-profile governmental figures, whether or not they actually interact with the federal research agencies. The Trump administration is historically unpopular among highly educated Americans, presumably including most scientists and researchers. See "In Changing U.S. Electorate, Race and Education Remain Stark Dividing Lines," Pew Research Center, June 2, 2020, https://www.pewresearch.org/politics/2020/06/02/in-changing-u-s-electorate-race-and-education-remain-stark-dividing-lines/.
[41] See Figure 1.

[42] H. Holden Thorp, "Do Us a Favor," *Science*, March 11, 2020, https://science.sciencemag.org/content/sci/early/2020/03/11/science.abb6502.full.pdf. See generally "Chapter 2: Perspectives on the Place of Science in Society," Pew Research Center, January 29, 2015, https://www.pewresearch.org/science/2015/01/29/chapter-2-perspectives-on-the-place-of-science-in-society/ ("Fully 83% of AAAS scientists say that getting government funding in their specialty area is harder today than it was five years ago[.]").

[43] See, e.g., Laura Sullivan and Cat Schuknecht, "Chinese Hacking Steals Billions; U.S. Businesses Turn A Blind Eye," *PBS Frontline*, April 12, 2019, https://www.pbs.org/wgbh/frontline/article/chinese-hacking-steals-billions-u-s-businesses-turn-a-blind-eye; Erik Sherman, "One in Five U.S. Companies Say China Has Stolen Their Intellectual Property," *Fortune*, March 1, 2019, https://fortune.com/2019/03/01/china-ip-theft/; Ellen Nakashima, "Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say," *The Washington Post*, May 20, 2013, https://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767_story.html.

[44] See, e.g., JASON, "Fundamental Research Security," 2.

[45] See, e.g., Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, "Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base" (C4ADS, 2019), 10, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d95fb48a0bfc672d825e346/1570110297719/Open+Arms.pdf; Sullivan and Schuknecht, "Chinese Hacking Steals Billions." See generally "Member Survey: US-China Business Council" (US-China Business Council, 2020), 13-14, https://www.uschina.org/sites/default/files/uscbc_member_survey_2020.pdf.

[46] Strengthening the U.S. government's broader open source intelligence capabilities would make this much more feasible, and is an important goal in its own right. See Chhabra et al, "Open-Source Intelligence for S&T Analysis."

[47] National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, 113 Stat. 1846 (2019), https://www.govinfo.gov/content/pkg/PLAW-116publ92/html/PLAW-116publ92.htm (available at https://www.congress.gov/bill/116th-congress/senate-bill/1790/text). In other cases, private-public groups have convened to produce reports such as "Fostering Integrity in Research" (The National Academies of Sciences, Engineering,

and Medicine, 2017), https://consortium.umn.edu/sites/consortium.umn.edu/files/fostering_research_integrity_nasem1.pdf. See also U.S. Senate Permanent Subcommittee on Investigations, *Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans* (Washington, DC: U.S. Senate Committee on Homeland Security and Governmental Affairs, 2019), 95-99 (discussing past and current collaborations involving the FBI), https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China%27s%20Talent%20Recruitment%20Plans%20Updated2.pdf.

[48] The National Cyber-Forensics and Training Alliance, https://www.ncfta.net/.

[49] Id.; "Here's How You Get Companies to Talk to Law Enforcement," *TAG Cyber Law Journal*; Nicole Hong, "Private-Public Collaboration Puts Pittsburgh at Fore of Cybercrime Fight," *The Wall Street Journal*, August 13, 2015, https://www.wsj.com/articles/private-public-collaboration-puts-pittsburgh-at-fore-of-cybercrime-fight-1439508624.

[50] "About ISACs," National Council of ISACs, https://www.nationalisacs.org/about-isacs; Jaikumar Vijayan, "What is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security," CSO, July 9, 2019, https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html; Sonner Kehrt, "The Cyber-Avengers Protecting Hospitals from Ransomware," *WIRED*, September 29, 2020, https://www.wired.com/story/cyber-avengers-protecting-hospitals-ransomware/.

[51] Vijayan, "What is an ISAC or ISAO?"

[52] See, e.g., "About Us," Institute of Nuclear Power Operations, http://www.inpo.info/AboutUs.htm; Financial Industry Regulatory Authority, https://www.finra.org. For discussion of similar trends in a different context, see Michael P. Vandenbergh, "Private Environmental Governance," *Cornell Law Review* 99, no. 1 (November 2013), https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=4615&context=clr.

[53] See, e.g., Joseph V. Rees, *Hostages of Each Other: The Transformation of Nuclear Safety Since Three Mile Island* (Illinois: University of Chicago Press, 1996). For a nuanced assessment of the financial industry's leading self-regulatory organization, see Joe Mont, "Market Shifts, SEC Priorities Spark Debate of FINRA's Future," *Compliance Week*, April 19, 2016, https://www.complianceweek.com/market-shifts-sec-priorities-spark-debate-of-finras-future/3054.article.