Business and Politics (2022), **24**, 113–132
doi:10.1017/bap.2022.2

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Inoculating the University R&D Enterprise: How RISC can strengthen post-COVID-19 research integrity and global supply chains

William J. Norris[1]*, Katie Vaughan-Naron[2], Neha Kashyap[3] and Joseph Balmain Rodgers[4†]

[1]Associate Professor and Director of the Economic Statecraft Program at the Bush School of Government and Public Service, Texas A&M University, College Station, TX, USA, 77843-4220, [2]Program Aide, Bush School of Government and Public Service, Texas A&M University, College Station, TX, USA, 77843-4220, [3]Graduate Student, Bush School of Government and Public Service, Texas A&M University, College Station, TX, USA, 77843-4220 and [4]Research Assistant, Economic Statecraft Program at the Bush School of Government and Public Service, Texas A&M University, College Station, TX, USA, 77843-4220
***Corresponding author:** William J. Norris, Email: economicstatecraft@tamu.edu

Abstract

The COVID-19 pandemic has underscored emerging vulnerabilities in the US research and development (R&D) ecosystem. While an open and collaborative environment has been essential for advancing R&D, this approach exposes university-based R&D to a variety of security threats including state-supported efforts, attacks by malicious actors, and insufficient internal mitigation. As the pandemic led to more remote work and online collaboration, the incidence of exploitation has expanded. Increased security measures are needed to insulate and protect the R&D ecosystem, and US innovation more broadly, while maintaining the fundamental qualities that have contributed to its historical success. In this article, we present the Research Integrity Security Certification (RISC) framework. This concept preserves the autonomy of the US higher education system while also suggesting a mechanism whose effect would be a general enhancement of the security of the US university R&D enterprise with minimal additional state involvement. Much of the work in the proposed model is done by market mechanisms and self-interested microeconomic calculations that generate beneficial aggregate effects. The RISC framework modernizes the university R&D enterprise while strengthening it to operate in this evolving security environment.

Keywords: RISC; supply chain; research integrity; innovation; research and development

Introduction

For more than a century, the United States has fostered the most advanced innovation ecosystem in the world. At the heart of the US research and development (R&D) enterprise lies its university-based research system. Rooted in strong ethical values such as objectivity, honesty, fairness, and stewardship, the university research system has embraced a structure of openness that contrasts with the closed nature of many research enterprises seen in rival nations.[1] This spirit of open collaboration has been essential in facilitating the innovation that has given the United States a global competitive edge since the post–World War II era and generated invaluable knowledge.

The American innovation ecosystem is increasingly under threat. In recent years, foreign actors have targeted and appropriated US intellectual property and research data for personal, commercial, and political gain. The onset of the coronavirus pandemic witnessed an escalation in these attacks. R&D efforts seeded by American universities provide invaluable catalysts for wider innovation and research, therefore it is crucial to protect the university R&D enterprise. This illuminates the core

[†]The authors wish to thank Ruben Mendoza, Ted Tyler, Ryan Sullivan, and Emily Ashbridge.

[1]Ostry and Nelson (1995), 37–39.

challenge facing the R&D ecosystem: How can the US higher education R&D enterprise be made more secure without eroding the characteristics that have underpinned its historical success?

In this article, we provide an overview of the challenges facing American universities' R&D enterprise in the post-COVID-19 world and sketch out a framework for protecting it. The first half of this piece addresses the importance of—and the need for—increased security across the US R&D enterprise by providing historical precedents, recent case studies, and relevant examples. Next, we analyze existing models used to protect against cyber threats and how to build on these to address ongoing challenges. We then propose a research integrity security certification (RISC) framework that could reinforce and strengthen the country's innovation base while preserving academic freedom and other key elements that characterize the university R&D enterprise.

National innovation systems and government relations

National innovation systems are often at the mercy of not only a nation's institutional development but also its policy decisions that direct the evolution of the R&D enterprise.[2] Techno-nationalism seems to be reemerging in countries where priority is being placed on government direction of dual-use and national security–related technology and innovation.[3] The techno-nationalism of Japan during the 1980s illustrated how competition with the United States drove scientific and technological investment and overall policy progress.[4] Similar dynamics may be emerging today in the United States–China relationship.

The American innovation ecosystem has played an important role in contributing to national security since World War II. While World War I's War Industries Board demonstrated the importance of industrial innovation for military strength, it was World War II's reinforced connection between R&D and national security that created the foundations for modern government policies toward innovation today.[5] The onset of World War II witnessed a rapid increase in government funding for university research to strengthen warfighting capacity. Through the Office of War Mobilization, formed in 1943 to coordinate the US war efforts, government funds funneled into critical defense sectors that spanned from aeronautics to biomedical trauma technology. This shift underscores how investment in R&D strengthens military capacities and can turn the tides of conflict and global competition.[6]

During the Cold War, the US innovation ecosystem again proved to be one of America's greatest strategic and economic strengths. Collaboration between the US government, academia, and technology sectors formed the basis of a national defense state in which security concerns motivated and focused support for innovation.[7] Spurred on by the Sputnik shock, post–World War II government support for R&D continued to swell as the United States strived for technological superiority over the Soviet Union across a wide range of fields.[8]

In addition to federal support, the US innovation ecosystem has been able to thrive due to its openness.[9] American scientists and engineers prided themselves on their willingness and ability to

[2]Mowery (2009), 455–57; Aggarwal and Reddie (2020).

[3]As defined by Richard Samuels (1994), ix, techno-nationalism refers to "the belief that technology is a fundamental element in national security, that it must be indigenized, diffused, and nurtured to make a nation rich and strong." For a recent treatment of this trend see Aggarwal and Reddie (2019), 40–47.

[4]Japan has long pursued the "tradition of maximizing military technological autonomy to maximize national strategic autonomy" as part of its grand strategy. A key feature of this is to promote indigenous production (*kokusanka*) while pursuing intersections of civilian and military production when possible. For more information, see https://warwick.ac.uk/fac/soc/pais/people/hughes/researchandpublications/articles/hughes_the_slow_death_of_japanese_techno-nationalism_jss_june_2011.pdf.

[5]Examples of this World War II period of innovation included: radar being developed at MIT; the Manhattan Project that involved leading academics from around the country; and British academics playing a key part in helping to break German encryption.

[6]Ostry and Nelson (1995), 34–36.

[7]Weiss (2014).

[8]Mowery and Rosenberg (1993), 29–75.

[9]An "open" research environment can be defined by "researchers hav[ing] low-cost and independent access to prior discoveries and research tools." For more on openness, see Murray et al. (2016).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

collaborate with other researchers across the nation and the world while frequently publicizing their discoveries. US President Ronald Reagan affirmed the importance of scientific cooperation by issuing National Security Decision Directive 189, which stated that "to the maximum extent possible, the products of fundamental research [are to] remain unrestricted."[10] Reagan, like other policy makers, understood the importance of openness and how the benefits of the free exchange of ideas outweighed the risk of US adversaries acquiring some advantages. In contrast, the Soviet Union's R&D and economic growth was limited by a lack of innovation diffusion, stunted private consumption and wages, and an incentive system that was resistant to technological change and innovations.[11] Russian science and technology, both under the centrally planned and transition economies, lagged behind the rest of the world and expended tremendous resources to catch up.[12] Comparatively, the virtue of openness secured the US innovation ecosystem and remains a pillar of its success that attracts the most talented students and researchers from around the world.

Investments that originated during this time ensured that the United States remained a leader in technology for more than fifty years.[13] The university-based R&D enterprise that has grown up around these Cold War efforts has remained an essential underpinning of national security innovation and economic primacy ever since. Now, the United States faces a rising threat from global competitors pursuing technological innovation and investment in their own indigenous R&D growth.[14]

The US research and development enterprise comprises nearly 25 percent of all global R&D spending and ranks tenth in R&D spending as a percentage of gross domestic product (GDP).[15] The United States spends more in absolute terms on R&D than any other nation, seeding an ecosystem that has produced many of the most significant advances in science and technology in the past century.[16] However, the People's Republic of China (PRC) is catching up rapidly with its own substantial investments in R&D. Chinese spending on innovation nearly doubled between 2003 and 2012 with China accounting for 32 percent of total global growth in R&D spending between 2000 and 2017.[17] Released in 2015, China's "Made in China 2025" plan calls for state and industry sources to invest in cutting-edge, advanced technologies that will bolster the domestic Chinese economy.[18] The release of the 14th Five-Year plan in March 2021 further outlines the PRC's drive to exponentially bolster its own R&D investments beyond that of any other global power. If the PRC succeeds with the commitments outlined in these strategic documents, it could unseat the United States as the world's economic and technological superpower.[19]

Even as Chinese R&D investments have grown, US federal investment in innovation and manufacturing has declined. The percentage of GDP spent on R&D dropped from 2 percent in the 1970s to only 0.7 percent by 2018. While private-sector funding for R&D has increased during these years, the private sector lacks the will and appetite to replace the foundational, basic research-supporting role historically played by the federal government.[20]

The US government has already recognized the central role it must play. In 2017, the White House included the National Security Innovation Base (NSIB) in its National Security Strategy, explicitly stating the need to "defend [America's] NSIB against competitors," and that losing technologies originating in universities would have "far-reaching negative implications for American prosperity and power."[21] The National Strategy for Critical and Emerging Technologies echoes this concern by identifying potential vulnerabilities for intellectual property theft and foreign espionage in early-stage

[10]Lane (2001).
[11]Aslund (2013), 17–21.
[12]Ibid.
[13]Weiss (2014).
[14]Manyika and McRaven (2019), 9.
[15]Valavanidis and Vlachogianni (2016), 9.
[16]Mowery and Rosenberg (1993), 29–75.
[17]Valavanidis and Vlachogianni (2016), 7; Khan et al. (2020).
[18]Kennedy (2015).
[19]Cheng (2021); Xinhua News Agency (新华社), Etcetera Language Group, Inc., and Murphy (2021).
[20]Manyika and McRaven (2019), vi–viii.
[21]The White House (2017), 21.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

technological development. To protect US primacy in innovation, Congress recently passed the United States Innovation and Competition Act of 2021 (USICA) allocating $110 billion for basic and advanced technology research across a five-year period.[22] With heightened research security and deliberate funding, the United States will be better prepared to protect its R&D enterprises and meet the global strategic concerns of the twenty-first century.

Ensuring the balance between security measures that protect R&D and an open and accessible environment essential for collaboration and innovation lies at the core of challenges facing the US R&D ecosystem. Openness and accessibility facilitate collaboration that is the lifeblood of the entire R&D community, but inherently create vulnerabilities that foreign actors have taken advantage of and continue to exploit. The government recognizes this balance. In a January 2021 memo, the Office for Science and Technology Policy (OSTP) called on the government to better secure the US research enterprise while "reducing innovation-killing administrative burdens."[23] While the Biden administration intends to enact many of the changes and policies suggested in the OSTP memo, maintaining a balance between security and openness will be the central challenge in sustaining US primacy in R&D and innovation.[24]

Dimensions of the COVID-19 impact

Recent developments related to COVID-19 have exacerbated many of these concerns about the integrity and longer-term sustainability of the nation's R&D enterprise, specifically at the university level. The sudden onset of the coronavirus pandemic disrupted global supply chains and impacted the university R&D enterprise in three significant ways: (1) transnational collaboration broke down, (2) remote work increased cyber vulnerabilities and insider risk, and (3) COVID-19 related R&D was targeted by state actors.

Barriers to transnational collaboration

Following the onset of the coronavirus pandemic, the collaborative ethos typically characterizing international public health coordination broke down amid growing tensions between strategic competitors. During the pandemic, international scientific collaboration on research, vaccine development, and information sharing should have been a top priority, yet many countries responded with a reflexively nationalistic and obstructive mentality.[25] Why did countries turn inward when cooperation was most needed? When their security is threatened, countries often fall back on what international relations scholars would call "realist" tendencies, pursuing their self-interests and naturally prioritizing the well-being of their citizens first.[26] During the pandemic, this effect would hinder transnational collaboration.[27] Such realist instincts worked against cooperative, transnational scientific collaborations to address the challenges posed by the pandemic.[28] Instead, some states have attempted to use their vaccine production as a critical form of global influence through vaccine diplomacy, leveraging life-saving R&D for geopolitical gain.[29] Even within the European Union, various individual countries chose to hoard critical medical supplies and shut down their borders. Countries turned inward when cooperation was of the greatest importance and transnational collaboration, a central tenet of innovation, deteriorated.[30]

China's response in the early stages of the pandemic exemplify the breakdown in transnational collaboration. In the critical months preceding the global spread of the coronavirus, China prevented

[22]Schumer (2021); The White House (2020), 9–10.
[23]Office of Science and Technology Policy (2020).
[24]Mervis (2021).
[25]Abbas (2020).
[26]Donnelly (2004), 7.
[27]Moloney (2020).
[28]Hafner et al. (2020), iii, 5–7.
[29]Conteh-Morgan (2021), 265–78.
[30]The Associated Press NBC News (2020).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

international epidemiological cooperation to address the outbreaks in Wuhan and opted to obfuscate knowledge of the virus until mid-January 2020. The World Health Organization (WHO) sent requests for data, but did not receive any response. Despite the growth in Chinese cases from late 2019 to early 2020, detailed data was kept from becoming common knowledge, and Beijing officials did not agree to work with an international team of experts until the end of January.[31] Chinese leadership seems to have been primarily focused on how their handling of COVID-19 would be perceived both domestically and internationally.[32]

China's aversion to information sharing and collaboration during the early stages of the pandemic was likely colored by ongoing strategic competition with the United States.[33] Since the 2010s, global unease has centered around United States–China competition. Under Xi Jinping, China had been gaining confidence on the world stage and COVID-19 offered an opportunity to further trumpet the benefits of the "China Model."[34] The COVID-19 crisis also sharpened the downward trend in relations between Washington and Beijing.[35] Growing distrust that characterized this rivalry made collaboration increasingly difficult. Complications surrounding tariff-driven trade wars and the placement of restrictions on sensitive technology sectors created additional barriers for collaboration.

As the state of the pandemic worsened, competition between the two nations escalated, with matters of vaccine nationalism and vaccine diplomacy representing a new feature of the long-standing bout.[36] As with the 2009 H1N1 virus, the coronavirus pandemic witnessed nations turning inward, securing their domestic populations and interests at the expense of global coordination. In addition to hindering multilateral cooperation, vaccine nationalism presented opportunities for misuse. For example, there is a risk that countries might bypass standards and regulations to "fast-track" vaccine distribution domestically.[37] In an attempt to outperform a competitor, countries may have been tempted to rush the development of a vaccine for their domestic population or for global distribution to garner geopolitical glory.[38] Vaccine nationalism not only threatened responsible R&D practices but also strained global supply chains. Logistically, supporting supply chains require multiple manufacturing steps, often across transnational borders. Vaccine production relies on global supply chains, while distribution requires international cooperation.[39] Most importantly, the breakdown in transnational collaboration in developing and distributing vaccines has left large swathes of the globe vulnerable to COVID-19 and its deadly side effects.

Although the next section demonstrates the need to develop a more comprehensive security system to prevent cyber threats, modifications to the R&D system should not prohibit international cooperation. As demonstrated in the preceding text, nations pursued vaccine diplomacy amid COVID-19 at the expense of the well-being of people while international cooperation should have been prioritized. The RISC framework we propose later is able to address vulnerabilities in the current system while also facilitating international exchanges to produce the best and brightest innovation ideas, especially in great times of need such as the COVID-19 global pandemic.

Increase in cyber vulnerabilities and insider risk

With the onset of the coronavirus pandemic and the shift to work from home, individuals, businesses, and government entities became more vulnerable to cyberattack threats.[40] This happened for two

[31]Ibid.

[32]Roy (2020); Ameyaw-Brobbey (2021), 172–90; Yeophantong and Shih (2021), 549; Wen (2021, February), 55–90; Yang and Chen (2021), 89–113.

[33]Wong (2021), 587–99.

[34]Wen (2021, February), 55–90.

[35]deLisle (2021, February), 231–56.

[36]Lin (2021), 139–68; Lee (2021), 1–15; Boylan et al. (2021, March), 23–40.

[37]Lipworth et al. (2020), 555–61.

[38]Burki (2020), 85–86.

[39]Hafner et al. (2020), iii, 5–7.

[40]State and nonstate actors as well as compromised insiders are targeting the data capital domain at an unparalleled rate when compared to the other R&D domains such as human capital. See, Muncaster (2020).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

reasons. First, the volume of online traffic increased as people spent a greater amount of time online.[41] This type of remote work increases opportunities for insider risks because there is necessarily more unsupervised access to sensitive information away from the place of work. Second, the volume of data in motion proliferated as data transferred between the office and home networks. Both shifts created greater opportunity for exploitation and hacking.

In the wake of increased vulnerabilities, malicious actors have employed an expansive toolkit targeting the US university R&D ecosystem. Exploitation techniques, such as phishing or social engineering campaigns in the cyber domain highlight the dangerous seams posed by insufficient security measures characteristic of a porous cyberspace.

The leading cause of breaches in the early months of the pandemic were directed phishing campaigns. Phishing campaigns lead to unauthorized access to systems and networks or result in widespread credential harvesting.[42] Once an attacker or group has access into the network, they can implement ransomware, which is often used to lock down database information until victims pay.[43] During the initial year of the pandemic, hackers increased targeting of prominent R&D institutions with ransomware to obtain lucrative intellectual property, such as COVID-related research, and money.[44] In June 2020, malicious actors launched a ransomware attack on researchers at the University of California in San Francisco (UCSF) who were conducting leading COVID-19 antibody testing research and clinical trials for possible treatments. Accidental insider risk facilitated the attack's success, as the stolen data was not backed up correctly by the researchers. This lapse in data stewardship by the researchers allowed the ransomware to infiltrate the team's network and steal sensitive data.[45] This is just one example of the many cyberattacks that targeted major research institutions with ties to epidemiology and COVID-related R&D. An intensification and escalation of these attacks exploited inherent vulnerabilities within the R&D ecosystem. Without necessary adjustments to in-house security protocols, future attacks may severely halt or setback life-saving research.

Another example of supply chain exploitation in the cyber domain was uncovered by IBM. In September 2020, IBM's new threat intelligence task force identified a global COVID-19 phishing campaign that spanned across six countries. Upon further investigation, the IBM team discovered that the attack's organizers were impersonating affiliation with the Vaccine Alliance's Cold Chain Equipment Optimization Platform (CCEOP), a vaccine distribution program. Had the attack been successful, the global response to COVID-19 would have been severely hampered.[46] Unfortunately, this example speaks to a broader trend in targeting high-value, high-stakes entities. In a similar case, IBM uncovered another phishing campaign against the personal protective equipment (PPE) supply chain. If successful, the global consequences would have once again been deadly. These recurring phishing campaigns demonstrate the increased use and danger of social engineering tactics targeting the R&D enterprise.[47]

Cases of COVID-19 R&D theft by state actors

Weakened by the coronavirus pandemic, countries from across the globe looked to American universities and innovation industries to gain illicit access to sensitive research. Various nations such as China, Russia, North Korea, and Iran exploited known vulnerabilities in the US R&D ecosystem to garner a strategic advantage in the race to respond to COVID-19. By breaching cyberspace defenses, state-actors can acquire critical (and often expensively produced) intellectual property without expending their own domestic resources. Federal Bureau of Investigation (FBI) and Homeland Security officials warned universities about the increasing number of cyberattacks coming from foreign

[41]Morgan and Sargent (2020).
[42]Ibid.
[43]Conklin et al. (2018), 77.
[44]Mehrotra (2020a).
[45]Mehrotra (2020b).
[46]Zaboeva and Frydrych (2020).
[47]Zaboeva (2020).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

countries.[48] Foreign government hackers primarily utilize known vulnerabilities that the target has not yet patched rather than searching for new avenues to exploit. By doing so, foreign actors maximize the potential impact of their activities while utilizing minimal resources. With countries like China and Russia testing weaknesses in an institution's computer infrastructure on a daily basis, cybersecurity shortcomings of potential targets are on full display.[49]

The United States views China as a main culprit in cyberattacks targeting US researchers. In May 2020, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) issued a formal warning to research institutions about Chinese attempts to target and steal COVID-19 research and information.[50] In July 2020, the US Department of Justice charged and indicted two Chinese hackers backed by the Ministry of State Security (MSS), China's civilian intelligence agency.[51] During July 2020, the US State Department ordered China to close its Houston consulate under allegations of R&D espionage. The consulate allegedly targeted and attempted to steal data from the University of Texas (UT) MD Anderson Cancer Center and the Texas A&M University System.[52] In the week following the closure, the FBI notified the UT campuses in both Austin and San Antonio, Texas, of potential biomedical research theft attempts being coordinated by the Chinese government.[53]

China is not alone in these attempts to subvert and profit from US R&D efforts toward pandemic-related research. Russia's intelligence services have targeted the United States, United Kingdom, and Canadian vaccine research networks. The British government first discovered Russian espionage efforts to obtain vaccine information and related research from the University of Oxford and its corporate partner, AstraZeneca. The report identified vaccine-related espionage efforts conducted by "Cozy Bear," an infamous Russian hacking group affiliated with Russia's foreign intelligence service.[54] These cyberattacks allowed Russia, like China, to access shortcuts in their pandemic-related R&D efforts, advancing their geopolitical efforts to be seen as effectively combating COVID-19.

North Korea and Iran have also attempted to obtain sensitive data primarily through the use of phishing emails directed at institutions engaging in the vaccine R&D. One group posed as the WHO and sent emails to medical researchers requesting a COVID-19 progress update. Another approach showed North Korean groups "phishing" these same individuals but under the guise of being a recruiter and offering fake job offers to the researchers.[55] Meanwhile, Iran targeted hacks toward pharmaceutical companies to obtain research data. Staff from the American drug company Gilead Sciences, Inc. reported thousands of Iranian email phishing attacks attempting to gain unauthorized access to the staff's email accounts.[56] These varied attempts at theft and access, especially when successful, hinder the overall global response efforts and illustrate some of the R&D ecosystem's vulnerabilities.

The heart of the problem

Research institutions in the United States possess unique, advantageous qualities such as openness, meritocracy, a culture of collaboration, transparency, sharing of information, and the relentless pursuit of cumulative knowledge. Some of these features have also been exploited and targeted, making universities vulnerable. Recent evidence suggests that these problems have become more acute. As research

[48]Federal Bureau of Investigation, Cyber Division (2021); Wolf and Gray (2010); the Department of Homeland Security linked Wolf and Gray's memorandum to their website to inform how universities should respond to data breaches. https://www.dhs.gov/cyber-incidents.

[49]Barnes and Venutolo-Mantovani (2020).

[50]FBI and CISA (2020).

[51]Lucas (2020).

[52]Moritsugu and Lee (2020).

[53]Britto (2020).

[54]Barnes and Venutolo-Mantovani (2020).

[55]Pressman (2020).

[56]Stubbs and Bing (2020).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

institutions adapt to a changing post-COVID-19 world, the security of these institutions may need improvements that do not jeopardize those qualities that make them effective.

This poses the delicate dilemma at the heart of securing the nation's university R&D enterprise: How can the university R&D enterprise be made more secure without eroding the characteristics that underpin its success? A sustainable solution to the security challenges must improve the system's integrity while preserving the key features that have made the US university R&D enterprise among the best in the world. In the sections that follow, we examine various existing models that hold promise before introducing our own proposal for how to approach this challenge.

There are four main channels related to research and development endeavors that will require the most attention to improve security: (1) physical assets, (2) human capital, (3) data integrity, and (4) external linkages. Efforts across each of these channels are necessary to protect the R&D enterprise. Physical assets include efforts to secure the physical research facilities, labs, and equipment. These often include security restrictions and measures that govern how these facilities are operated, constructed, maintained, and verified. Human capital refers to those individuals that are granted access to facilities and sensitive data. Data integrity focuses on the accuracy, completeness, and reliability of the creation, storage, and transmission of data. It emphasizes the potential danger of sensitive data loss from insider and foreign threats. Finally, external linkages are formal or informal contacts, relationships, or agreements individuals or institutions have with external organizations or individuals. External links are central characteristics of the research enterprise, but they also come with a certain level of risk. This risk is enhanced when the collaboration is transnational and not well-vetted. Malign collaborating individuals or institutions pose a final source of threat to the integrity of the university R&D enterprise. Improved defenses across each of these four dimensions will help ensure R&D organizations reach their full potential while ensuring their integrity.

Existing models that seek to enhance enterprise security

Recently, several models have emerged to enhance security in the research and innovation supply chain space. The most promising of these proposals rely on incentivizing and encouraging institutions that conduct sensitive R&D to obtain a certain level of security. While these models are helpful improvements in defensive measures, the continuing theft of intellectual property across the university R&D enterprise suggests the need for additional work on this challenge.

Cybersecurity Maturity Model Certification

The Cybersecurity Maturity Model Certification (CMMC) is a leading approach that ensures all defense industrial base (DIB) contractors meet cybersecurity requirements for handling controlled unclassified information.[57] The CMMC is built around US government standards and regulations, using those incentive structures to shape the evolution of defense industry suppliers. The CMMC was created in coordination with Department of Defense (DoD) stakeholders and, notably, University Affiliated Research Centers (UARCs) and Federally Funded Research and Development Centers (FFRDC) to strengthen the security of the DIB and the supply chain of the DoD.[58] The CMMC uses a maturity model to measure an institution's cybersecurity robustness based on its adherence to security frameworks when responding to various threats.[59] The CMMC uses existing federal regulations to guide its framework for 171 best cybersecurity practices and five maturity processes.[60]

[57]To view a list of Frequently Asked Questions about the CMMC, see "Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification FAQs," Office of the Under Secretary of Defense for Acquisition & Sustainment (2020e).

[58]Office of the Under Secretary of Defense for Acquisition & Sustainment (2020a).

[59]According to the CMMC Version 1.02, a maturity model is "a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline." Office of the Under Secretary of Defense for Acquisition & Sustainment (2020b).

[60]Office of the Undersecretary of Defense for Acquisition & Sustainment (2020b), 10.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

The CMMC provides a standardized level of certification to DIB contractors. Receiving this certification assures the DoD that a contractor can respond appropriately to a specific level of risk. Therefore, DIB contractors are encouraged to become certified to retain contract work.[61] Yet, a large obstacle to wider DIB adoption is the high upfront cost of certification. Small and medium-sized enterprises comprise a majority of the DIB. Such small and medium-sized enterprises often lack the necessary funds for advanced security measures and certifications because they frequently depend upon their cash profits to sustain operations or continued growth.[62] Up-front, fixed costs are more easily absorbed by larger enterprises that can spread such costs over a bigger revenue base.

The CMMC has five levels of cyber hygiene practice, each with its own criteria: basic, intermediate, good, proactive, and advanced. The corresponding processes are performed, documented, managed, reviewed, and optimized, respectively. Both the process and practice requirements must be fulfilled to achieve a certain level, and uneven capabilities between the two certifies the organization at the lower level.[63] In essence, organizations at the basic cyber hygiene level safeguard federal contract information (FCI), and progress to the intermediate level as a transition step toward protecting controlled unclassified information (CUI) as required by the "good" level.[64] Organizations at the proactive and advanced levels protect CUI and reduce risk of advanced persistent threats (APTs).[65] Although the CMMC mainly focuses on cybersecurity, it includes seventeen diverse domains including asset management, personnel security, physical protection, and system and communications protection. These types of domains correspond to the physical assets, human capital, data integrity, and external linkages categories suggested earlier. While the CMMC model focuses on protecting industry, our RISC proposal (discussed in the following text) would help secure university settings. RISC is designed to address both cyber and noncyber threats in the research environment.

Global Engagement Risk Assessment and Management Program

The Global Engagement Risk Assessment and Management Program (GERAMP) created by Kevin Gamache and Glenn Tiffert provides an adherence framework for research institutions to combat research theft and restore research integrity. The basic steps that GERAMP identifies and encourages research institutions to adopt are: know your partners, know your funders, take contracts seriously, train, iterate, and adapt.[66] Reiterating the problems and vulnerabilities associated with permissiveness in the research and development enterprise, Gamache and Tiffert's model underscores the pervasive exploitation of research institutions by the PRC. While GERAMP begins to address some of the challenges facing universities, much of the GERAMP approach is rooted in central university administration. For example, Gamache and Tiffert suggest the creation of a GERO (Global Engagement Review Office) to ensure administrative leadership and coordination for GERAMP.[67] While administrative leadership ensures the coordination of operations, there is an important grassroots component to preventing research theft: the individual principal investigators (PIs). In the RISC prototype discussed in the following text, we explicitly seek an inclusive approach that seeks to leverage the incentives and autonomy of researcher units.

[61]Ibid., 1–2.

[62]Norris et al. (2020), 65–81.

[63]For more information on the origin of the inspiration for these processes as well as an extensive list of each level's requirements, see Office of the Under Secretary of Defense for Acquisition & Sustainment (2020b).

[64]For more information on the level-one examination process and requirements, see "CMMC Assessment Guide Level 1," Office of the Under Secretary of Defense for Acquisition & Sustainment (2020c), https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf. For more information on level three, see "CMMC Assessment Guide Level 3," Office of the Under Secretary of Defense for Acquisition & Sustainment (2020d), https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf.

[65]The CMMC Assessment Guide for Level Two has been skipped due to its status as an optional, intermediate phase. The CMMC Assessment Guide for Levels Four and Five will be released at an undetermined later date.

[66]Tiffert and Gamache (2020), 113–15.

[67]Ibid., 122.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Although RISC similarly leverages a certification level system, our proposal focuses on three distinctive characteristics. First, researchers opt-in to our system that allows them to retain their autonomy and preserves agency for the academy (an important feature of any long-term solution). This is quite different from the case-by-case enforcement that dominates the existing approach for securing higher education R&D. Second, our solution is systemic and capitalizes on the already existing natural incentive structures rather than struggling against them. Our approach avoids the impression of arbitrary enforcement to address these challenges. Piecemeal discretionary efforts often skirt racially problematic profiling and are not always grounded in the known empirics that inform risk models. Third, our approach is fundamentally proactive rather than reactive. Our proposal would proactively assess risk as a condition of access to sensitive research. By limiting risk at the front end, our model seeks to *prevent* compromises of the university R&D enterprise rather than relying on detection and ex-post punishment and deterrent rationales. Ultimately this is a much more sound and strategic approach that can move beyond reactive strategies that necessarily lag behind the threat.

Outlines of the Research Integrity System Certification: A prototype to inoculate the university R&D enterprise

The university R&D enterprise has unique features and properties that ought to be incorporated into a successful effort to enhance its security. Our contribution is to preserve the autonomy of the US higher education system while also suggesting a mechanism whose theoretical effect would be a general enhancement of the security of the US university R&D enterprise with minimal additional state involvement. Importantly, the RISC framework capitalizes on the natural incentives of the constituent actors to improve the overall, systemic level of security. The innovative RISC proposal outlined in the text that follows prioritizes working within the organically occurring incentive structure of higher education to harness individual actors' optimization in a way that produces aggregate outcomes that make the overall university R&D enterprise more secure. Similar to both the CMMC and the GERAMP frameworks, our RISC approach is based on distinct levels of certification. Individual university labs and research groups would be certified on a 1–5 scale depending on security measures across each of the four dimensions presented earlier: physical assets, human capital, data integrity, and external links/collaboration categories. Universities include a range of unique features and actors that distinguish them from industry and any successful effort to enhance security of the university R&D enterprise will require working collaboratively *with* these characteristics and incentives rather than against them or in an oppositional manner.

RISC offers several benefits. First, adoption will be completely voluntary. Individual labs and research groups can decide whether they would like to participate and at what level. The freedom of researchers to opt-in preserves the autonomy and agency of academia. The specific level of certification an individual lab selects will depend on the nature of their work and the sort of grants the laboratory is seeking. Second, the preventative, systemic approach that RISC adopts would be an improvement over the current case-by-case enforcement paradigm. Current efforts are necessarily retrospective and fundamentally punitive in nature. Third, opting-in would be incentive-driven rather than compliance-driven. Abiding by higher levels of integrity certification would qualify a particular lab to compete for certain types of grants and federal contracts. For example, grants awarded in sensitive or dual-use technologies could begin to require a level 4 or above integrity certification. This would incentivize research groups or labs to adopt measures that would ensure they had the appropriate security practices in place to qualify to apply for the grant. Rather than orienting the mechanism around an oppositional compliance approach, RISC capitalizes on the alignment of incentives. Fourth, this proposed system preserves the freedom, flexibility, and agency of higher education entities. Individual PIs and their research groups could self-select into whatever level of security was optimal for their work. Academia bristles at what has become seen as government overreach and infringement on academic freedom and autonomy. RISC offers the advantage of preserving the agency of academic researchers and institutions. Fifth, RISC addresses the problem of high upfront costs by leveraging resources of larger entities that would be better positioned to absorb upfront, fixed costs.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Smaller-scale institutions could join a research consortium with larger players. These larger organizations would be better placed to engage in the certification process and more easily provide the associated overhead. As an affiliated partner, researchers from the smaller school could benefit from the capabilities of the consortium. Programs that encourage smaller (often less-well-endowed) minority-serving institutions to partner with larger, R-1 research universities already exist today. Such consortia are often well-positioned to compete for federal grant programs. Larger institutions would have the incentives and resources to not jeopardize their RISC rating. Such programs would thus help researchers from smaller schools overcome the issue of upfront costs while also ensuring that smaller partners benefitted from robust institutional support. In other words, larger institutions risk assuming liability from the vulnerabilities of their smaller partners, so they are motivated to provide the resources necessary to ensure that the "weakest link" in their supply chain does not compromise their security. During the initial RISC pilot implementations, these collaborative dynamics will be tested with the intention of making adjustments as lessons are learned. Finally, the RISC system would open the possibility for better trusted collaboration venues that would be reserved for access by scholars at certain certification levels (e.g., a journal only accessible to researchers certified at level four or above). These would facilitate intellectual exchange among scholars while preserving some degree of operational security.[68]

To ensure a fair and consistent certification grading system, a dedicated, stand-alone body would be needed. Congress could authorize this body to assess and award RISC certifications. To achieve practical scale, this body may need subordinate regional entities capable of evaluating various labs in its jurisdiction. This new certifying entity would be in charge of setting the standards and requisites within each security level. Research institutions would have the ability to perform internal assessments and decide the importance of increased security. Individual institutions would determine when upgrades are warranted given potential funding opportunities. The National Institute of Standards and Technology (NIST) Special Publication 800-171 Rev. 2 addresses the standards for handling CUI at the federal level.[69] Similar to the GERAMP model, all RISC standards will comply with the NIST 800-171 requirements to ensure that certified research institutions can automatically meet any federally sponsored research criteria.[70] Having this requirement as a built-in standard in the RISC system allows research institutions to opt-in with fewer worries about qualifying for federal research grants. Federal grant providers can set a specific qualifying level based on the research being conducted and then choose a qualified institution. This certification process allows federal entities to feel more secure in choosing a specific partner institution when sensitive unclassified national security-related research and development is involved.

Details of the RISC model's five levels will ultimately be shaped by the voices of multiple stakeholders. Each certification level's standards will be based upon recommendations from US research institutions. Because there could be many additional considerations or factors that have not been adequately anticipated, it will be important to roll out RISC through pilot programs that can allow for feedback, learning, adaptation, and enhancement. Involving the public sector, the private sector, and academia achieves more realistic and transparent security standards that work for all parties involved. Broad participation better ensures that RISC meets all the stakeholders' needs. Rather than having only academic researchers or government agencies unilaterally design the requirements for each level, we suggest involving multiple stakeholders in the prototype design. Ensuring that multiple parties discuss the certification criteria helps the model better represent the enterprise makeup. It also reinforces adoption and makes the model more adaptable as feedback from pilot rollouts is incorporated.

Once certification requirements at the various levels are set, certifications will be assessed across the four dimensions of research integrity, with clearly defined requirements corresponding to each level of certification. Higher levels of certification (4 or 5) should be reevaluated quarterly, given the potential

[68]We are indebted to one of the anonymous reviewers for this idea.
[69]National Institute of Standards and Technology (2020).
[70]Tiffert and Gamache (2020), 120.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

for rapidly evolving threat vectors, while it is sufficient to conduct lower levels of certification on an annual basis. The accrediting body could allow university administrators to annually self-assess and self-certify the university's own labs and groups at the first two security levels—an internal security assurance process. But higher levels of certification would entail external assessments and would need to be certified by the stand-alone RISC authority created by Congress. Decentralizing the lowest levels to universities relieves the burden on auditors to investigate entities at all levels. Auditors will be able to focus on higher-level certifications. Universities would need to have attained lower levels of certification prior to submitting for higher level certification. This design retains the institutional ability to self-assess threats, risks, and countermeasures. This requires continual risk and threat assessments, threat or risk classification, and then assessing if the countermeasures in place are successfully mitigating them. These steps will be a periodic process that, over time, builds institutional capacity. Such localized capacity will also aid an institution's attempts to increase its security and certification level.

The resulting "race to the top" dynamics

Creating national security standards throughout the R&D enterprise will likely begin a "race to the top" effect among US research institutions, which could lead to higher security levels across the national university R&D enterprise system. The RISC model will be systemic and capitalize on natural incentive structures rather than trying to fight them. Introducing the RISC would likely trigger what David Vogel deemed "The California Effect" in 1995. In Vogel's classic example, California was granted the option to create stricter emissions standards than the national level. In 1970, the state accepted this proposal and adopted some of the toughest vehicle emissions standards seen up to that time. Because California was a large and growing consumer market for cars, the auto industry elected to produce vehicles that met California's stringent requirements. If cars met the California standards, they would exceed all of the other states' vehicle emissions requirements. Thus, Detroit produced cars that could be sold in California (and thus everywhere else as well). Rather than running two separate assembly lines to make both cleaner cars that met the California standards and legacy cars that met lower standards, the producers simply shifted production to the higher California standards. This decision was less expensive than producing two (or more) versions of the same model car. Once the manufacturers built a more efficient engine, it did not make business sense to continue producing the inferior version.

The resulting systemwide effect was that the state of California unilaterally raised emissions standards nationwide. This new and stricter standard was soon codified by the US Congress in 1990 to officially become the national emissions standard. A new baseline was set. Yet again, California was permitted to elevate its standards above that of the nation. California did. Following California's decision, other states were given the option to choose their emissions standards: the lower national level or the higher California standards. Twelve eastern states requested for their standards to match California's standards in 1994. In this example, Congress allowed the implementation of a more liberal policy, and other states subscribed to California's standards. Consequently, the individual decisions of states led to the de facto increase of overall national standards.[71] Once again, microeconomic rationales of auto plants led to the effective nationwide adoption of California's more stringent standards.

The aggregate effect was a ratcheting up of vehicle emissions standards in the United States—not primarily by heavy-handed federal regulation, but rather by a "race to the top" dynamic in which a large state market required higher standards as the price for market access. Microeconomic incentives made the use of different assembly lines to meet different standards unattractive in terms of profitability. Various plants around the nation switched to more stringent vehicle standards because it was more efficient. Essentially, microeconomic optimization took care of vehicle emission standards in a way that still allowed carmakers to retain their autonomy. Similarly, even if only a handful of key R1 research universities initially adopt RISC, as long as the main funding sources began introducing RISC requirements into a handful of the most cutting-edge arenas, the results would be dramatic. Universities that

[71]Vogel (1995), 322.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

were more reluctant to adopt such standards would suddenly be incentivized to reverse their behavior once confronted with contracts in leading technological areas being awarded to other universities that have adopted RISC standards.

Once NIH, NSF, and DoD grants and contracts at the frontiers of science, medicine, and engineering research begin opening sensitive proposals only to labs or groups possessing certain RISC certifications, the effect would lead to even wider adoption. Leading universities that might not have been initially enthusiastic might seek to participate. The resulting aggregate outcome would be a "race to the top" effect where others would follow suit. Within a relatively short period, the most valuable, sensitive, or strategic parts of the university R&D enterprise could be efficiently elevated to a higher level of security. The mechanism for this transformative industry-wide effect is primarily driven by the prospect that an institution could find itself limited by its low security certification. Institutions that adopt higher security standards would experience an advantage in the awarding of federal contracts. Those that are more reluctant to embrace these measures would miss future opportunities. Achieving certain levels of certification would enable a given lab to be eligible to compete for NSF, DOD, or NIH calls that are restricted (e.g., needing a level 3 or higher). Reaching higher levels effectively creates a "revenue" offset to the additional incurred costs of shoring up an institution's security. Institutions will need to weigh the benefits against the costs of enhanced security. It is clear that any security enhancements will entail some sort of costs. Our RISC prototype provides a sustainable market-based mechanism for shouldering those costs. Alternatively, universities might elect to do nothing and remain vulnerable. In that case, there is a good chance that a security "solution" would be imposed upon academia. Such a solution is unlikely to prioritize academic autonomy or choice.

Rather than mandate compliance, the RISC's advantage is its voluntary and incentive-driven nature. Research institutions are likely to pursue certification to improve their competitiveness for certain grants. In the process, the system's overall security will be enhanced. Economist Charles Tiebout developed a theory that demonstrates economic efficiency through a household's decision to live in a specific location out of the desire to consume specific local goods.[72] Tiebout sorting can be observed when a family decides to buy a specific house based on the corresponding school district. An older, retired couple whose children are already grown may choose to avoid buying a house in that district given the higher property taxes and little use for schools at their stage of life. Instead, they opt for a house in a nearby town with lower taxes. However, both households are better off because of a diversity of supply that lets them "opt-in" to their preferred location. In this example, Tiebout underscores how mobile families "vote with their feet" and will choose to live in a location based on the presence of local commodities that align with the family's preferences.[73]

In a similar fashion, as the government searches for partner institutions to conduct leading work in critical and emerging areas, it will "vote with its funding" and provide the most secure institutions with the grant funding. As the institutions with a lower rating observe federal contracts and grants being given to the institutions with a higher security rating, the incentive becomes desirable, and a broad-based elevation in the security of university R&D will eventually result. If some institutions elect to err on the side of less security in favor of continued unfettered openness and collaboration, they may continue to do so. These more vulnerable parts of the university R&D enterprise will no longer be in possession of the most attractive dual-use technologies or strategically valuable data. Like the older couple, this is not a "bad" outcome. It simply reflects a differing utility function. The RISC system allows individual labs and research groups to self-select into the most appropriate level of research security given their needs. Individual researchers can also be permitted to move from labs with higher or lower security protocols in place, thus "voting with their feet." Different institutions will prefer differing levels of security. Heterogeneity will not only create a more secure research environment within the United States but it will also prove beneficial for both parties involved: the research institution in question and the grant provider.

[72]Tiebout (1956), 416–24.
[73]Brunner (2014), 62.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Elements of the R&D enterprise to protect

As Gamache and Tiffert's research points out, the US R&D enterprise must develop an adequate response strategy to combat research integrity threats. Otherwise, the US government may step in with uncoordinated and more restrictive alternatives.[74] Keeping this in mind, we propose a framework for assessing the research integrity of a given lab or research group.[75] To arrive at a security level certification, we suggest assessing and grading a given lab's safeguards and procedures across four domains: physical assets, human capital, data integrity, and external links. Improvements to security must complement the unique features of the US higher education and the research ecosystem. Some of these qualities include openness and transnational collaboration linkages (the large number of foreign graduate students, faculty, and researchers, peer institution collaborations, funding sources, etc.). These features have played a significant role in successfully propelling the US research enterprise and need to be accommodated in any sustainable security-enhancing effort.[76]

Physical asset security

While hacking and cyberattacks often receive the most attention, they are not the only methods by which sensitive information can be stolen or accessed. The security of physical facilities and equipment is also an important component of ensuring the safety of the R&D enterprise. Physical asset security can cover facilities, their internal infrastructure, security features (both physical and digital), and data.[77] As David Hutter highlights in a SANS Institute report, the primary objective of physical security is to safeguard an institute's personnel, information, equipment, IT infrastructure, facilities, and any related assets.[78]

Because data is stored and accessed through physical entities, physical security and procedures are the first lines of defense and mitigation against data loss. Similar to the CMMC model that provides institutional standards for cybersecurity, physical security should also be assessed and provided with a level grade. The assessment and its requirements for each level will be made transparent to institutions applying for the certification, ensuring the standards and levels are known and attainable. Based on this goal of certification clarity, pilot sectors will be rolled out in institutions shown to be high risk for R&D targeting. These pilot sectors will be the testing ground for this RISC process. Early testing ensures the RISC parameters are least likely to hinder collaboration and scientific progress at the chosen institutions and laboratories. By first testing this system at a smaller scale, initial feedback and results can be quickly obtained, specific processes easily tweaked, and new insights applied to specific R&D enterprise members. Lessons learned will then be incorporated before rolling out the RISC system more broadly. This allows stakeholders to provide input and voice their concerns. Ultimately the desired outcome of this model is to transition R&D communities into a higher level of security segmentation regarding unclassified data and research security.

Human capital

Foreign talent enhances the creativity and innovation within R&D by providing a diverse set of experience, capabilities, and perspectives. The United States remains the destination of choice for the top scientists and engineers from around the world. It would be harmful to cut off this vibrant pipeline of talent.[79] Jill Welch, the former Deputy Executive Director for the Association of International

[74]Tiffert and Gamache (2020), 13.

[75]The RISC framework would apply solely to unclassified information. Classified material is outside the scope of this proposed system and would continue to be handled in the university R&D setting in the same way it is done today.

[76]JASON and MITRE Corporation (2019)

[77]One potential unintended result of creating stronger data protection could be an increase in cyber espionage. While cybersecurity is a part of the RISC model, displacement toward cyber vulnerabilities could result from improvements to universities' physical and human capital security. This concern will be watched during the pilot phase using empirical data that can identify any unexpected displacement of threat to the cyber domain.

[78]Hutter (2016), 1.

[79]Krige (2014).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Educators, testified that policies that portray the United States as isolationist or unwelcoming of international students should be avoided, or else we risk "shooting ourselves in the foot."[80] Since the onset of COVID-19, and with the rise in nationalism at a global scale, the attitude toward hiring non-US citizens has become more hostile. Rather than a facile blanket approach that drifts toward xenophobic tendencies, RISC would emphasize the need for professional vetting of individuals that would work on sensitive technologies.

Thorough background and security checks should be the minimum standard for personnel criteria if the research institution plans to receive a federal grant or contract in a sensitive area. Only those doctoral students who desire to work in a lab that holds a high level of certification through the RISC system will be required to undergo a background check. Most doctoral students complete coursework during the first one to two years of a program, which is an ideal time to go through the background check process. Completing this process before moving into the research phase that follows will enable doctoral candidates to work in any of the labs that hold stricter certification levels. The National Strategy for Critical and Emerging Technologies calls for the balancing of valuable contributions of foreign researchers with "fostering research security in academic institutions, laboratories, and industry."[81] Indeed, improved security measures and foreign researchers are not mutually exclusive. Rather, the security risk that any individual poses is what ultimately matters. In 2006, 43 percent of all PhDs were awarded to students on temporary visas, and the ten-year retention rate of PhD recipients was 58 percent.[82] Even amidst a complex visa and citizenship system, there is a strong desire among doctoral degree recipients to live and work in the United States that any security model should acknowledge. Instead of dismissing this foreign talent, policy makers and security models should incentivize integration of foreign talent into the US innovation ecosystem. This means improving processes like background checks for all personnel, US citizens and noncitizens alike. While foreign ties can be a risk factor, there is a danger in falling into a deceptively simple dichotomy that assesses risk solely on citizenship. Labs should make all personnel aware of the standards and security protocols to which they will be held and conduct the vetting and periodic reviews appropriately. When breaches do occur, full details and characteristics of the case should be factored into future screening efforts.

Data integrity

Data integrity can be parsed into five components, each of which deserves consideration in the effort to certify the integrity of data.[83] The first involves the generation, production, or coding of data. Then consideration ought to be given as to how the data is stored, uploaded, and compiled. What are those procedures, and how secure are they? Third, integrity involves how data is accessed, analyzed, and exported from its storage domain into its manipulation domain. Fourth, data integrity involves how data can be extracted, downloaded, copied, or moved within the lab or user group. Fifth, consideration needs to be given to how the data is sent, shared, transmitted, or accessed to and from the outside. This last aspect also involves the transmission infrastructure addressed in the physical asset domain above.

The COVID-19 pandemic underscored the threat cyberattacks pose to the preservation of data integrity within the R&D environment, especially as remote work increased. In 2017, accidental insider threats from employees, contractors, researchers, and others accounted for 25 percent of all data breaches.[84] Not only are the actions of remote workers already more difficult to monitor but also many of these cyberattacks were directed at any access-holding end-user regardless of the location. These attack methods highlight the risks and the results of accidental insider threats. To increase data security, routine personnel training is needed. Research institutions should ensure that all

[80]Welch and NAFSA: Association of International Educators (2018).

[81]The White House (2020), 9.

[82]Stephan (2010), chapt. 10.

[83]Addressed during the Bush School Economic Statecraft Program's Meeting Notes with Texas A&M University's Chief Information Officer, Mark Stone, on November 18, 2020.

[84]McKee (2018).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

personnel know what accidental data misuse and access looks like, the warning signs, and how to prevent it where possible. Implementing a policy of "dual person access" could be a potential mitigation strategy. This policy would require more than one authorized person to access an organization's sensitive data. The downside of this method, especially with the increase in remote work, is the time delay imposed on the work environment. As with many security measures, the security benefit could potentially outweigh the inconveniences if the data were sensitive enough. Forcing a person to request sensitive data with another authorized person could help prevent intentional insider threats and deter theft. Our suggestion for RISC's standards would be to have training and awareness as the minimum-security requisite. Additional measures could be installed for higher-level certifications, pending industry and pilot program feedback.

External links and collaboration

Collaboration can be with individuals or institutions. External links also include sources of funding and other forms of compensation. Formal and informal collaboration between the United States and foreign entities seems to be the primary mechanism through which improper influence is exerted across the research enterprise. A MITRE Corporation's report lists six categories that stakeholders recognize as problematic in the realm of external linkages: theft (of intellectual property, methods, and data), failure to disclose a connection, use of improper foreign talent programs, espionage, conflict of commitment, and conflict of interest. Each activity can occur through formal or informal R&D collaboration and opens up any connected party to increased risk.[85] Increased security would enable researchers to collaborate more safely with counterparts worldwide thus maximizing scientific and creative potential. When assessing the extent of foreign collaboration within the research environment, it is important to remember that risk will never be fully avoidable. However, the benefits will often outweigh the vulnerabilities. If research institutions want to address these challenges with foreign collaboration, then the dissemination of security information and knowledge will be key.

Countries like China use talent programs to target professionals and researchers for the purposes of achieving technology transfer and gaining sensitive data access. These programs offer money, job opportunities, and other incentives to obtain desired knowledge or technology.[86] US research personnel should be kept up to date with information concerning foreign talent programs. Important information would include what research is being targeted, the primary modus operandi of various countries, and the red flags that need to be identified and reported. Ensuring that personnel can recognize these recruitment attempts and reporting any witnessed attempts are the minimum standards to reinforce and strengthen the human capital dimension.

RISC pilot implementation should begin by developing prototypes in the four or five most vulnerable sectors. The evaluation of this limited RISC rollout should indicate if economic espionage and the loss of sensitive data were reduced, and whether implementation improves US research competitiveness. This pilot rollout will be implemented in sectors most critical to national security concerns and in those sectors most targeted by foreign actors (e.g., sectors like aerospace, biopharmaceuticals, and semiconductors). It would be appropriate to conduct a cost-benefit analysis for the key actors to better understand how the RISC's proposed incentive structures would work in practice. These pilot sectors could demonstrate the RISC model's efficacy in areas where the status quo protections have been insufficient. Such pilot projects ought to be studied to understand what elements of the RISC concept ought to be adjusted or enhanced. Rather than speculate, we encourage prototype trials to surface any unanticipated outcomes and adapt the system design accordingly. If the RISC model proves its worth in these pilot sectors, then it could be expanded as an innovative effort to reduce technology loss and transfer.

[85]Ide et al. (2020), 2, 11.
[86]Joske (2020), 12.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Conclusion

American innovation has not only propelled the US economy and military forward, but it has helped raise standards of living worldwide. These gains have been made possible by a robust R&D ecosystem that unites public, private, and academic institutions into a dynamic force for innovation. Maintaining this competitive edge is essential for ensuring that the US continues to lead advancements in science and technology. Despite historical and institutional advantages, emerging threats from state and non-state adversaries as well as declining investment trends in basic research risk placing the US R&D ecosystem on a downward spiral.

While the open and collaborative US R&D environment facilitates innovation, it provides tempting opportunities for cyberattacks and other vectors of exploitation to acquire intellectual property and sensitive data.[87] Given academia's vulnerabilities, it is unsurprising that global competitors regularly target university R&D enterprises to acquire IP and sensitive data. The US university R&D environment will remain a prime target of foreign exploitation until these vulnerabilities are shored up.

Considering that the United States is already a leader in many R&D sectors, this proposal seeks to reverse the erosion of this dominant position. The RISC approach moves away from the arbitrariness of current enforcement efforts to secure the R&D enterprise. Piecemeal discretionary enforcement often problematically resembles profiling based on nationality and is not always grounded in the empirics of risk models. Every individual carries the potential for a security breach regardless of nationality or ethnicity, and RISC addresses this by strengthening background checks across the board. RISC is fundamentally proactive rather than reactive. RISC assesses security concerns up front as a condition of access to sensitive research.

The university research and development enterprise undergirds broader US innovation and ingenuity. Providing a certification system into which individual labs can self-select will allow research enterprises and grant providers to benefit from overall improvement and increased security measures across all dimensions of R&D, from data integrity to global supply chains. As the myriad of threats that target fundamental research and innovation continue to grow, ensuring a more secure post-COVID-19 research environment should remain a priority in the decades ahead.

References

Abbas, Muhammad Zaheer. 2020. "Practical Implications of 'Vaccine Nationalism': A Short-Sighted and Risky Approach in Response to COVID-19." Research Paper No. 124. South Centre. https://www.google.com/url?q=http://hdl.handle.net/10419/232250&sa=D&source=docs&ust=1636759872700000&usg=AOvVaw2tD_irAa8lm6m1VfxTXlyn.

Aggarwal, Vinod K., and Andrew W. Reddie. 2019. "Regulators Join Tech Rivalry with National-Security Blocks on Cross-Border Investment." *Global Asia* 14 (1): 40–47.

Aggarwal, Vinod K., and Andrew W. Reddie. 2020, August. "Security of Supply: The Determinants of State Intervention in Emerging Technology Sectors." *Asia Global Papers* 3: 1–38.

Ameyaw-Brobbey, T. 2021. "A Lost Chance for What? COVID-19 and Its Repercussions on Global Public Opinion of China's Development Model and International Leadership." *Journal of International Studies* 14(3): 172–90. https://doi.org/10.14254/2071-8330.2021/14-3/11.

Aslund, Anders. 2013. *How Capitalism Was Built: The Transformation of Central and Eastern Europe, Russia, the Caucasus, and Central Asia*. Cambridge University Press.

Associated Press, The. 2020. "How China Blocked WHO and Chinese Scientists Early in Coronavirus Outbreak." *NBC News*. https://www.nbcnews.com/health/health-news/how-china-blocked-who-chinese-scientists-early-coronavirus-outbreak-n1222246.

Barnes, Julian E., and Michael Venutolo-Mantovani. 2020. "Race for Coronavirus Vaccine Pits Spy Against Spy." *New York Times*. Race for Coronavirus Vaccine Pits Spy Against Spy - The New York Times (nytimes.com).

Boylan, Brandon M., Jerry McBeath, and Bo Wang. 2021. "US–China Relations: Nationalism, the Trade War, and COVID-19." *Fudan Journal of the Humanities and Social Sciences* 14 (1): 23–40. https://doi.org/10.1007/s40647-020-00302-6.

Britto, Brittany. 2020. "FBI Looking into Possible Chinese Spying on UT's COVID Research." *Houston Chronicle*. https://www.houstonchronicle.com/news/houston-texas/education/article/FBI-Chinese-spy-COVID-university-texas-austin-15446341.php.

Brunner, Eric J. 2014. "School Quality, School Choice, and Residential Mobility." In Ingram, Gregory K. and Daphne A. Kenyon (eds.) *Education, Land, and Location* (Cambridge, MA: Lincoln Institute of Land Policy): 62–87.

Burki, Tala. 2020, September. "The Russian Vaccine for COVID-19." *The Lancet Respiratory Medicine* 8 (11): 85–86. https://doi.org/10.1016/S2213-2600(20)30402-1.

[87]Barnes and Venutolo-Mantovani (2020).

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Cheng, Jonathan. 2021. "China Is the Only Major Economy to Report Economic Growth for 2020." *Wall Street Journal*. https://www.wsj.com/articles/china-is-the-only-major-economy-to-report-economic-growth-for-2020-11610936187.

Conklin, Wm. Arthur, Greg White, Chuck Cothren, Roger L. Davis, and Dwayne Williams. 2018. *Principles of Computer Security: CompTIA Security+ and Beyond*, 5th ed. McGraw-Hill Education.

Conteh-Morgan, Earl. 2021. "Strategies of Sino-American Rivalry in Africa: From 2000 to COVID-19." *Vestnik RUDN International Relations* 21 (2): 265–78. https://doi.org/10.22363/2313-0660-2021-21-2-265-278.

deLisle, Jacques. 2021, February. "When the Fever Breaks? COVID-19, US-China Relations, and East Asia." *Orbis* 65 (2): 231–56. https://www.sciencedirect.com/science/article/pii/S0030438721000053.

Donnelly, Jack. 2004. *Realism and International Relations*. Cambridge University Press.

FBI and CISA. 2020. "People's Republic of China (PRC) Targeting of COVID-19 Research Organizations." https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.

Federal Bureau of Investigation, Cyber Division. 2021. "Increase in PYSA Ransomware Targeting Education Institutions." *FBI Flash*. https://www.ic3.gov/Media/News/2021/210316.pdf.

Hafner, Marco, Eerez Yerushalmi, Clement Fays, Eliane Dufresne, and Christian Van Stolk. 2020. "COVID-19 and the Cost of Vaccine Nationalism." *RAND Research Report RR-A769-1*. DOI: https://doi.org/10.7249/RRA769-1. https://www.rand.org/pubs/research_reports/RRA769-1.html.

Hutter, David. 2016. "Physical Security and Why It Is Important." *SANS Institute White Paper*: 1–30.

Ide, Lisa M., Karen F. Lee, Brittini A. Fine, Christopher S. Moeller, Dr. Daniela Silitra, Dr. Jodi L. Simco, Alex Sisti, and Adam L. Terragnoli. 2020. "Improper Influence in Federally Funded Fundamental Research." *MITRE Corporation Technical Paper*: 2, 11. https://www.mitre.org/sites/default/files/publications/pr-20-3351-improper-influence-in-federally-funded-fundamental-research.pdf.

JASON and The MITRE Corporation. 2019. "Fundamental Research Security." https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

Joske, Alex. 2020. "Hunting the Phoenix, the Chinese Communist Party's Global Search for Technology and Talent." Australian Strategic Policy Institute ASPI, Policy Brief Report No. 35. https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-10/Hunting%20the%20phoenix_v2.pdf?VersionId=TX_kD_pNKlBF.xuSdZO1UMuTKmiNEeAK.

Kennedy, Scott. 2015. "Made in China 2025." *Center for Strategic & International Studies*. https://www.csis.org/analysis/made-china-2025.

Khan, Beethika, Carol Robbins, Abigail Okrent. 2020. "The State of US Science and Engineering 2020: Global R&D." National Science Foundation. National Science Board. https://ncses.nsf.gov/pubs/nsb20201/global-r-d.

Krige, John. 2014. "National Security and Academia: Regulating the International Circulation of Knowledge." *Bulletin of the Atomic Scientists* 70 (2): 42–52. https://doi.org/10.1177/0096340214523249.

Lane, Neal. 2001. "The Openness Imperative." *Foreign Policy*, April, 80–81. 224049555. ABI/INFORM Collection; Military Database; PAIS Index; Worldwide Political Science Abstracts. https://www.proquest.com/magazines/openness-imperative/docview/224049555/se-2?accountid=7082.

Lee, Seow Ting. 2021. "Vaccine Diplomacy: Nation Branding and China's COVID-19 Soft Power Play." *Place Branding and Public Diplomacy:* 1–15. https://doi.org/10.1057/s41254-021-00224-4.

Lin, H. Y. 2021. "COVID-19 and American Attitudes toward US-China Disputes." *Journal of Chinese Political Science* 26: 139–68. https://rdcu.be/cBm3c.

Lipworth, Wendy, Melanie Gentgall, Ian Kerridge, and Cameron Stewart. 2020, August. "Science at Warp Speed: Medical Research, Publication, and Translation during the COVID-19 Pandemic." *Journal of Bioethical Inquiry* 17: 555–61. https://doi.org/10.1007/s11673-020-10013-y.

Lucas, Ryan. 2020. "DOJ Charges 2 Suspected Chinese Hackers Who Allegedly Targeted COVID-19 Research." *NPR*. https://www.npr.org/2020/07/21/893832580/doj-charges-2-suspected-chinese-hackers-who-allegedly-targeted-covid-19-research.

Manyika, James, and William H. McRaven. 2019. "Innovation and National Security: Keeping Our Edge." Council on Foreign Relations. https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf.

McKee, Mike. 2018. "Accidental Insiders Pose a Serious Threat to Your Organization." *InfoSecurity*. https://www.infosecurity-magazine.com/opinions/accidental-insiders-serious-threat/.

Mehrotra, Kartikay. 2020a. "Hackers Target California University Leading Covid Research." *Bloomberg*. https://www.bloomberg.com/news/articles/2020-06-04/hackers-target-california-university-leading-covid-19-research.

Mehrotra, Kartikay. 2020b. "How Hackers Bled 118 Bitcoins Out of Covid Researchers in US." *Bloomberg*. https://www.bloomberg.com/news/features/2020-08-19/ucsf-hack-shows-evolving-risks-of-ransomware-in-the-covid-era.

Mervis, Jeffrey. 2021. "Parting Trump Memo on US Research Security Seen as Road Map for Biden." *Science and Policy*. https://doi.org/10.1126/science.abg8064;https://www.sciencemag.org/news/2021/01/parting-trump-memo-us-research-security-seen-road-map-biden.

Moloney, William. 2020. "Coronavirus Is Accelerating the Advance of Nationalism over Globalization." *The Hill*. https://thehill.com/opinion/international/492253-coronavirus-is-accelerating-the-advance-of-nationalism-over.

Morgan, Daniel, and John F. Sargent Jr. 2020. "Effects of COVID-19 on the Federal Research and Development Enterprise." Congressional Research Service Report, Summary and p. 1. Effects of COVID-19 on the Federal Research and Development Enterprise (congress.gov).

Moritsugu, Ken, and Matthew Lee. 2020. "US Ratchets Up China Tensions, Closing Houston Consulate." *AP News*. https://apnews.com/article/ffc84d09363ba0a1a0e6db3c05bb8322.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

Mowery, David C. 2009. "National Security and National Innovation Systems." *Journal of Technology Transfer* 34: 455–73. https://doi.org/10.1007/s10961-008-9100-4.

Mowery, David C., and Nathan Rosenberg. 1993. "The US National Innovation System." In: Nelson Richard R., (ed). *National Innovation Systems: A Comparative Analysis*. Oxford: Oxford University Press; 1993: 29–75.

Muncaster, Phil. 2020. "#COVID19 WFH Rules Ramp Up Phishing and Insider Risks." *InfoSecurity*. https://www.infosecurity-magazine.com/news/covid19-wfh-phishing-and-insider/

Murray, Fiona et al. 2016. "Of Mice and Academics: Examining the Effect of Openness on Innovation." *American Economic Journal: Economic Policy* 8 (1): 212–52. https://doi.org/10.1257/pol.20140062.

National Institute of Standards and Technology. 2020. "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

Norris, William J. et al. 2020. "A Market-Oriented Approach to Supply Chain Security." *Security Challenges* 16 (4): 65–81.

Office of Science and Technology Policy. 2020. "President Trump Takes Bold Action to Strengthen the Security and Integrity of America's Research and Development Enterprise." https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSC-OSTP-NSPM33-Fact-Sheet-Jan2021.pdf.

Office of the Under Secretary of Defense for Acquisition & Sustainment. 2020a. "Cybersecurity Maturity Model Certification (CMMC)." *Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification*. https://www.acq.osd.mil/cmmc/index.html.

Office of the Under Secretary of Defense for Acquisition & Sustainment. 2020b. "Cybersecurity Maturity Model Certification (CMMC) Version 1.02." *Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification*. https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

Office of the Under Secretary of Defense for Acquisition & Sustainment. 2020c. "CMMC Assessment Guide Level 1." *Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification*. https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf.

Office of the Under Secretary of Defense for Acquisition & Sustainment. 2020d. "CMMC Assessment Guide Level 3." *Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification*. https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf.

Office of the Under Secretary of Defense for Acquisition & Sustainment. 2020e. "CMMC FAQ." https://www.acq.osd.mil/cmmc/faq.html.

Ostry, Silvia, and Richard R. Nelson. 1995. *Techno-Nationalism and Techno-Globalism: Conflict and Cooperation*. Brookings Institution Press.

Pressman, Aaron. 2020. "Hackers Are Trying to Disrupt and Steal COVID-19 Vaccine Research." *Fortune*. https://fortune.com/2020/11/13/covid-vaccine-hackers-cyberattack-coronavirus-north-korea-russia/.

Roy, Denny. 2020. "China's Pandemic Diplomacy." *East-West Center*. No. 144. https://www.google.com/url?q=https://www.jstor.org/stable/pdf/resrep28881.pdf&sa=D&source=docs&ust=1636949452874000&usg=AOvVaw1FwLc7FqC3CUJ6Y8L96tRN.

Samuels, Richard J. 1994. "Rich Nation, Strong Army": National Security and the Technological Transformation of Japan. Cornell University Press.

Schumer, Charles E. 2021. *S.1260 - United States Innovation and Competition Act of 2021*. Congressional Bills, 117th Congress. U.S. Government Publishing Office.

Stephan, Paula. 2010. "The 'I'S' Have It: Immigration and Innovation, the Perspective from Academe." In: Josh Lerner and Scott Stern (eds.) *Innovation Policy and the Economy*. Volume 10. *National Bureau of Economic Research*: 83-127. https://doi.org/10.1086/605854.

Stubbs, Jack, and Christopher Bing. 2020. "Exclusive: Iran-linked Hackers Recently Targeted Coronavirus Drugmaker Gilead—Sources." *Reuters*. https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV.

Tiebout, Charles. 1956. "A Pure Theory of Local Expenditures." *Journal of Political Economy* 64 (5): 416–24.

Tiffert, Glenn, and Kevin Gamache. 2020. "Global Engagement: Rethinking Risk in the Research Enterprise." *The Hoover Institution*. https://www.hoover.org/sites/default/files/research/docs/tiffert_globalengagement_full_0818.pdf.

Valavanidis, Athanasios, and Thomais Vlachogianni. 2016. "Research and Development: The Role of Universities for the Knowledge-Based Society and Technological Innovations. Expenditure in Scientific Research and Applications as Crucial Factors for Economic Growth and the New Technological Frontiers." Website: www.Chem.Uoa.Gr *Scientific Reports, Department of Chemistry* (1): 1–39. https://www.researchgate.net/publication/310708656_Research_and_Development_The_Role_of_Universities_for_the_Knowledge-based_Society_and_Technological_Innovations_Expenditure_in_Scientic_Research_and_Applications_as_Crucial_Factors_for_Economic_Growth.

Vogel, David. 1995. *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Harvard University Press.

Weiss, Linda. 2014. *America Inc.? Innovation and Enterprise in the National Security State*. Cornell University Press.

Welch, Jill, and NAFSA: Association of International Educators. 2018. "Hearing on Student Visa Integrity: Protecting Educational Opportunity and National Security." Subcommittee on Border Security and Immigration. https://www.judiciary.senate.gov/imo/media/doc/Welch%20Testimony1.pdf.

Wen, Yao. 2021. "Branding and Legitimation: China's Party Diplomacy amid the COVID-19 Pandemic." *China Review* 21 (1): 55–90. https://www.jstor.org/stable/27005555.

White House, The. 2017. "National Security Strategy of the United States of America." https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

https://doi.org/10.1017/bap.2022.2 Published online by Cambridge University Press

White House, The. 2020. "National Strategy for Critical and Emerging Technologies." https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf.

Wolf, Christopher, and Tracy Gray. 2010. "University Responses to Breach of Data Security." *American Council on Education*. https://www.acenet.edu/Documents/University-Responses-to-Breach-of-Data-Security.pdf.

Wong, W. K. O. 2021. "Sino-Western Rivalry in the COVID-19 'Vaccine Wars': A Race to the Bottom?" *Asian Education and Development Studies* 10 (4): 587–99. https://www.emerald.com/insight/content/doi/10.1108/AEDS-12-2020-0271/full/html.

Xinhua News Agency (新华社), Etcetera Language Group, Inc., and Ben Murphy. 2021. "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." *Center for Security and Emerging Technology*. https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

Yang, Yifan, and Xuechen Chen. 2021. "Globalism or Nationalism? The Paradox of Chinese Official Discourse in the Context of the COVID-19 Outbreak." *Journal of Chinese Political Science* 26 (1): 89–113. https://www.google.com/url?q=https://doi.org/10.1007/s11366-020-09697-1&sa=D&source=docs&ust=1636949453687000&usg=AOvVaw3Stza-4mwEsbwfzVxeLFRf.

Yeophantong, Pichamon, and Chih-yu Shih. 2021. "A Relational Reflection on Pandemic Nationalism." *Journal of Chinese Political Science* 26 (3): 549. https://doi.org/10.1007/s11366-021-09736-5.

Zaboeva, Claire. 2020. "German Task Force for COVID-19 Medical Equipment Targeted in Ongoing Phishing Campaign." *Security Intelligence*. https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/.

Zaboeva, Claire, and Melissa Frydrych. 2020. "IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain." *Security Intelligence*. https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/.

Cite this article: Norris WJ, Vaughan-Naron K, Kashyap N, Rodgers JB (2022). Inoculating the University R&D Enterprise: How RISC can strengthen post-COVID-19 research integrity and global supply chains. *Business and Politics* **24**, 113–132. https://doi.org/10.1017/bap.2022.2