CHAPTER TWO

# Global Engagement: A New Paradigm for Managing Risk

KEVIN GAMACHE AND GLENN TIFFERT

## I. Introduction

American research institutions operate in a hyper-globalized environment with a wide degree of autonomy. This plays to their many strengths, but it also exposes them to risks that they are ill-equipped to handle. Chapter 1 of this report documents one urgent category of those risks, but there are a great many others that touch nearly every discipline of knowledge, including: censorship, espionage, IP theft, foreign surveillance and intimidation of US campus communities, and foreign interference in research and academic affairs.[1] Here we take up the question: What is to be done?

In general, the response to these risks has been to recommend better training and stricter compliance and to reach for incremental legislative or regulatory fixes. While prudent in a narrow sense, this approach

1. Glenn D. Tiffert, *Compromising the Knowledge Economy: Authoritarian Challenges to Independent Intellectual Inquiry*, National Endowment for Democracy, April 2020, https://www.ned.org/sharp-power-and-democratic-resilience-series-compromising-the-knowledge-economy; Anastasia Lloyd-Damnjanovic, "A Preliminary Study of PRC Political Influence and Interference Activities in American High Education," *Woodrow Wilson International Center for Scholars*, 2018, https://www.wilsoncenter.org/publication/preliminary-study-prc-political-influence-and-interference-activities-american-higher.

is nevertheless myopic, fragmented, and reactive. It obviates the need for strategic thinking, cedes the initiative, and keeps our institutions on the backfoot, ever playing catch-up.

Over time, the shortcomings of this approach have grown too obvious to ignore. Some risks are not responsive to compliance-driven remedies and therefore smolder, for instance self-censorship and the weaponization of student enrollments.[2] For others, successive regulatory measures have deposited layers of well-intentioned disclosure and reporting mandates, each with its own demands and destination. Likewise, lists drawn up by government agencies with different jurisdictions and missions impose a profusion of legal regimes on their enumerated entities and technologies. In the last several months alone, two more such lists have appeared on the horizon, courtesy of Section 1281 of the 2020 National Defense Authorization Act and Presidential Proclamation 10043.[3]

These interventions map unevenly onto a research enterprise that includes private firms, national laboratories, private universities, and multi-campus state university systems with diverse risk profiles and capacities. The cumulative result is a patchwork of poorly integrated, ill-fitting solutions that are updated irregularly, create gaps of their own, and make compliance progressively more burdensome and prone to failure. Even assuming perfect implementation, gains may be short-lived because determined adversaries can adapt faster than government rulemaking can keep pace, for instance by exploiting the spaces between

2. Sheena Chestnut Greitens and Rory Truex, "Repressive Experiences among China Scholars: New Evidence from Survey Data," *The China Quarterly*, 2019, 1–27, https://doi.org/10.1017/S0305741019000365; Tiffert, *Compromising the Knowledge Economy*, 6.

3. *National Defense Authorization Act for Fiscal Year 2020*, Public Law 116-92, § 1281; US President, "Proclamation 10043 of May 29, 2020: Suspension of Entry as Nonimmigrants of Certain Students and Researchers From the People's Republic of China," document 85 FR 34353, *Federal Register* 85, no. 108 (June 4, 2020), https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic.

the rules, obfuscating identities or working through surrogates.[4] The gains may also be illusory and breed complacency to the extent that such circumvention strategies succeed.

More to the point, this system can operate perfectly and still prejudice the interests of the United States.[5] As Chapter 1 has shown, research institutions are obliged to observe the law, but if the law marks a path for them to collaborate with a given entity, then they are free to take it irrespective of the ramifications for national security and economic competitiveness. Until June 5, 2020, only two of the PRC's Seven Sons of National Defense universities were on the Department of Commerce's Entity List, and while that number has since doubled, it hardly matters if the collaboration at issue falls within the list's fundamental research exemption. And the Seven Sons are just the tip of the spear; within the PRC alone there are dozens of other universities and research institutes at the national, provincial, and municipal levels that are deeply involved in military research, including some of the country's most highly-regarded universities, such as Tsinghua University and the University of Science and Technology of China.[6] Add in other countries like Russia and Iran, and the scope of the problem grows daunting.

We believe that continuing down the current road will yield diminishing returns and breed harmful dynamics between US research institutions and their regulators. In light of recent shifts in government policy, the

4. Linda Lew, "More 'Eyebrows on Fire': Another Chinese University Dodges Export Controls on US Software," *South China Morning Post*, June 25, 2020, https://www.scmp.com/news/china/diplomacy/article/3090615/more-eyebrows-fire-another-chinese-university-dodges-export?utm_source=copy_link&utm_medium=share_widget&utm_campaign=3090615.
5. Amy Hawkins, "Banned but Not Broken," *The Wire China*, May 31, 2020, https://www.thewirechina.com/2020/05/31/sensetimes-american-axis.
6. Alex Joske, *Picking Flowers, Making Honey; The Chinese Military's Collaboration with Foreign Universities*, Report No.10 (Canberra: Australian Strategic Policy Institute, 2018), https://www.aspi.org.au/report/picking-flowers-making-honey; Alex Joske, *The China Defence Universities Tracker*, Report No. 23 (Canberra: Australian Strategic Policy Institute, 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

discretion to pursue foreign engagements depends more than ever on new thinking—on research institutions reinventing their internal risk assessment and management processes to deliver higher quality, granular decisions. As evidence of foreign interference and exploitation accumulates in the research enterprise, external pressure to curtail its autonomy and openness in the name of national security and economic competitiveness will intensify, and bluntly prescriptive proposals will come increasingly to the fore. That outcome is avoidable, but only if we change the paradigm.

In this chapter, we propose the concept of a Global Engagement Risk Assessment & Management Program (GERAMP), which provides an organizational and operational framework for how research institutions should assess and manage foreign engagement risk. Second, we propose the establishment of a Global Engagement Review Office (GERO) to provide administrative leadership, oversight, and coordination of the GERAMP and to liaise with relevant federal entities. Third, and most fundamentally, we recommend that research institutions redefine their posture by adopting Operational Security (OPSEC) as the governing paradigm for foreign engagement risk. Fourth, we propose a Global Engagement Maturity Model (GEMM) through which institutions can formalize and optimize their internal capabilities to assess and manage foreign engagement risk. And fifth, we recommend the constitution of a new government-sponsored entity that would contribute unique research and analytic capacity on foreign engagement risk and establish a unified point of contact about it for the research enterprise.

## II. Key Principles and Commitments

The recommendations in this chapter are guided by and consistent with a set of principles and commitments that are fundamental to the manner in which the research enterprise operates in the United States. These principles and commitments include:

- *Institutional autonomy and openness.* Academic independence and open flows of people, information, and ideas are integral to the success of the US research enterprise.

- *Empowerment*. Empowering research institutions to manage their foreign engagements with greater rigor and better information is essential to upholding their autonomy and safeguarding research integrity and security.
- *Strategic competition*. It is not in the national interest for US research institutions to support the defense R&D or industrial base of strategic competitors such as the PRC, even if that research is designated fundamental and not subject to export controls or other restrictions pursuant to National Security Decision Directive (NSDD) 189.[7]
- *Values*. US institutions should not collaborate on research with entities that support the surveillance capabilities of authoritarian regimes or the capacity of those regimes to violate democratic values or human rights.
- *Unacceptable risks*. While foreign state-directed influence over US research and individuals recruited through foreign state talent programs are not synonymous with espionage or intellectual property theft, they represent unacceptable risks. These efforts serve national strategies to acquire sensitive US information and technology. Similarly, foreign activities targeting US research can threaten US national or economic security even if there is no involvement or control by a foreign state entity.
- *Inclusivity*. Strategic competitors, such as the PRC, co-opt, incentivize, direct, and/or coerce individuals to transfer technology and intellectual capital irrespective of the ethnicities and nationalities of those individuals. For instance, the PRC targets members of the ethnic Chinese diaspora, individuals who do not claim Chinese ethnicity, and PRC and US citizens alike *after* they obtain expertise and/or placement and access to critical US research or technologies. Focusing primarily on students and scholars in the

7. The White House, *White House Directive on Fundamental Research Exemption*, National Security Decision Directive-189, September 21, 1985, https://www.aau.edu/key-issues/nsdd-189-white-house-1985-directive-fundamental-research-exemption.

United States who are foreign nationals is therefore wholly inadequate to the relevant risks. Because any person can facilitate the unauthorized transfer of technology and intellectual capital, due diligence must be performed on every participant in a foreign research collaboration.

- *Transparency, integrity and reciprocity*. Research institutions should not compromise their standards of transparency, integrity, and reciprocity to facilitate foreign engagements. They must be prepared to pause, throttle back, or terminate engagements if those standards are not met.
- *Partnership*. Safeguarding national security and economic competitiveness are chiefly the responsibilities of the US government. Nonetheless, cooperation between research institutions and federal agencies is integral to the success of those efforts and can greatly enhance them.
- *Greater investment*. Increased US government funding for domestic research and innovation is necessary to safeguard research integrity and security. Strategic competitors, such as the PRC, will continue to offer opportunities to US entities that may not be in the long-term national interests of the United States. The US government and research sector must also devote greater effort to *domestic* commercialization of R&D.
- *Incentivized performance*. Government funding decisions should reward institutions that implement robust research integrity and security programs and penalize those that do not.

## III. Key Constraints

Foreign efforts to interfere with or exploit research activities can take many forms, from critical skills acquisition and espionage to funding arrangements that unduly influence the conduct of research, lead to the loss of future value, and erode control over intellectual property. However, serious constraints limit the capacities of the US government and US research institutions to assess and mitigate the risks posed by foreign engagements. These constraints include the following:

- *Disparate missions*. Research institutions and the government understand their missions and constituencies differently. This can generate friction, mistrust, and gaps in mutual understanding.
- *Incomplete tools*. Research institutions have not been sufficiently responsive to foreign engagement risks because they lack incentives to think outside of the box of their formal compliance mandates. Meanwhile, criminal law cannot compensate for a dearth of civil remedies because, strictly speaking, many risks do not lead to prosecutable crimes.[8] Absent a new paradigm, acute risks will continue to fall through the cracks.
- *Barriers to information sharing*. The US intelligence community relies heavily on classified information to identify threats posed by foreign entities. This severely limits its ability to share information with the research community. Likewise, the FBI and other federal law enforcement components are often unable or unwilling to share timely or sufficiently detailed information from investigations. Meanwhile, research institutions guard their autonomy and worry that involving law enforcement and the intelligence community in internal matters might redound upon vulnerable members of their communities and the climate for academic freedom.
- *Regulatory disorder*. Legal mandates and reporting requirements are often inconsistent, poorly coordinated, burdensome, and confusing. For instance, federal funding agencies may request the same or similar data in different ways, when uniform collection would be more reliable and efficient. Regulatory terms may also lack clear definitions, which compromises implementation.
- *Weak governance*. Some institutions or unauthorized personnel within them enter into foreign contracts and other commitments without first performing rigorous due diligence and risk assessments. Many also have weak compliance cultures that undermine

8. Margaret K. Lewis, "Criminalizing China," *Journal of Criminal Law and Criminology* 111, no. 1 (Seton Hall Public Law Research Paper, forthcoming 2020), https://ssrn.com/abstract=3600580.

the implementation of existing institutional policies and processes and impair the fulfillment of regulatory mandates.

- *Institutional incapacity*. The resources, domain knowledge, language skills, and leadership available to identify, evaluate, and manage the risks implicated in a lawful foreign engagement vary greatly from one research institution to another. It is unrealistic to expect ordinary administrators, research program managers, development officers, and grant reviewers to possess them in sufficient measure.
- *Governmental incapacity*. Area expertise, critical language skills, and the domain knowledge to make informed technical assessments of frontier science and technology are in short supply in government.[9] Rulemaking is fragmented and cumbersome, and lags behind the best available threat information. For instance, the US government has routinely issued visas to students and researchers to work in critical STEM fields who are directly tied to foreign military programs or other organizations on the Department of Commerce's Restricted Entity List. Research institutions may wrongly assume that the admitted individuals are low-risk.

## IV. Basic Steps for Addressing the Problem

Due diligence is the cornerstone of any risk assessment and management program. In the context of foreign engagements, institutions and researchers must ensure that all of the participants in a prospective collaboration are clearly documented irrespective of whether the collaboration will be formal or informal. They must also verify that the collaboration's nature, scope, and purpose are well-defined and transparent, consistent with relevant laws and regulations, undertaken with full knowledge and consent, and in a manner that avoids harm to core values and national interests. At a minimum, this requires robust commitments such as these:

9. Jude Blanchette and Seth G. Jones, "The U.S. Is Losing the Information War with China," *Wall Street Journal*, June 16, 2020, https://www.wsj.com/articles/the-u-s-is-losing-the-information-war-with-china-11592348246.

- *Know your partners.* Institutions and researchers must understand who their prospective partners are and not rely on how those partners represent themselves. Background research should draw on multiple information sources, in cooperation with government agencies as necessary. For an institutional partner, this will ordinarily include analysis of its past activities, the sectors it operates in or is associated with, its beneficial owners, and the commercial and ethical standing of its governing body.

  Vetting of individuals should determine whether an individual and their associates are from reputable organizations, possess relevant qualifications, and have any unexplained gaps or items of concern in their backgrounds. High-risk collaborators sometimes supply sanitized CVs that omit important publications, affiliations, and awards, or mistranslate them into English. Background research can bring more complete, native-language versions of their CVs to light. Searching their publication records in their native languages can also expose valuable information. The depth of this background research will depend on the nature of the collaboration, but it should include all of the key participants, not just the principal investigators, because experience has shown that graduate students and postdoctoral scholars are a significant threat vector. Insider threat is not limited by ethnicity, institutional affiliation or country of origin.
- *Know your funders.* Research institutions are struggling to manage the risk associated with sponsored research and philanthropic giving, and they are suffering significant reputational harm in the process.[10] Entanglements with Huawei and SenseTime in particular demonstrate poor due diligence and risk forecasting.[11] Sponsored research and philanthropic gifts open channels for foreign entities

10. Susan Svrluga, "Epstein's Donations to Universities Reveal a Painful Truth About Philanthropy," *Washington Post*, September 8, 2019, https://www.washingtonpost.com/local/education/epsteins-donations-to-universities-reveal-a-painful-truth-about-philanthropy/2019/09/04/e600adae-c86d-11e9-a4f3-c081a126de70_story.html.
11. Hawkins, "Banned but Not Broken."

to access and influence research and academic affairs and impinge on institutional autonomy.[12] The financial shock of COVID-19 has sharpened these vulnerabilities. Greater safeguards and stricter oversight, with formal representation from area and subject matter specialists who can put foreign funders into context, are broadly necessary.

- *Take contracts seriously*. A foreign entity may propose to formalize a collaboration using its own contract while the US partner may lack the legal training to adequately comprehend the terms of that document and its omissions. To protect their interests, institutions should adopt checklists and model templates to guide the negotiation of all collaboration agreements. Prior to signature, authorized personnel should review and approve the final texts to ensure that they satisfactorily address, as appropriate: dispute resolution; choice of law; governing language; potential threats to research integrity, intellectual property, and reputation; and applicable regulatory requirements and standards of data governance, ethics and human rights.[13]
- *Train*. Institutions should sensitize their personnel to potential risks when collaborating with a foreign partner, train them in

12. John Fitzgerald, "How Bob Carr Became China's Pawn," *Australian Financial Review*, November 8, 2018, https://www.afr.com/policy/what-you-should-know-about-bob-carr-and-china-20181105-h17jic; Primrose Riordan, "London School of Economics Academics Outraged by Proposed China Programme," *Financial Times*, October 27, 2019, https://www.ft.com/ content/2dd5ed50-f538-11e9-a79c-bc9acae3b654; Josh Rogin, "University Rejects Chinese Communist Party-linked Influence Efforts on Campus," *Washington Post*, January 14, 2018, https://www.washingtonpost.com/opinions/global-opinions/university-rejects-chinese-communist-party-linked-influence-efforts-on-campus/2018/01/14/c454b54e-f7de-11e7-beb6-c8d48830c54d_story.html; Gordon Lubold and Dustin Volz, "U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research," *Wall Street Journal*, May 14, 2020, https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205.

13. Frank Bekkers et al., "Checklist for Collaboration with Chinese Universities and Other Research Institutions," *HCSS Global Trends*, The Hague Centre for Strategic Studies, January 31, 2019, https://hcss.nl/report/checklist-collaboration-chinese-universities-and-other-research-institutions.

applicable laws, policies, and processes, and identify internal resources for assistance. For example, foreign partners may have undisclosed relationships, operate in different ethical and political environments, and be ignorant of US legal requirements. Observance of US norms governing informed consent and human subjects research may be uneven. Foreign state actors may reap project data and use it for unanticipated ends. Insiders may transfer technology and intellectual capital without proper authorization. Researchers should possess sufficient background information to weigh and prepare for those contingencies.

Informal collaborations are vital to the advancement of knowledge. They emanate from the freedom of inquiry, a core academic value that requires support. At the same time, informal collaborations present nontraditional intelligence collectors with soft targets for exploitation. Researchers must be vigilant against the risks that informal collaborations may present and act responsibly, ethically, and in good faith. Expanded Responsible Conduct of Research (RCR) training can help them to do so. It can also clarify the scope of a researcher's authority to enter into commitments and the processes to be followed in bringing a collaborative opportunity to fruition.

- *Iterate and adapt*. Laws, regulations and government policy evolve. Likewise, the scope of a collaboration, its participants, their behavior, and other circumstances may change, which can alter its original risk profile. Effective due diligence must periodically review ongoing collaborations and formal agreements, reevaluate risk, and adjust safeguards as necessary. It must also ensure that ongoing collaborations and formal agreements meet the latest guidance and legal requirements and bring them into compliance if they do not.

Foreign exploitation of the US research enterprise under the cover of lawful activity is a present danger.[14] Chapter 1 has shown that even

14. US Department of Justice, *Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions since 2018*, 2020, https://www.justice.gov/opa/page/file/1223496/download.

openly published research of a basic or fundamental character is susceptible to that threat. This should not surprise us. If the value of the American research enterprise was reducible to the information content of its published work, then most foreign students and scholars would never seek US partners; they would simply stay at home and read more. They seek collaboration to tap US resources, such as expertise, laboratories, and data, and to gain intangible benefits. In the United States, they can master the art of science through exposure to a highly successful culture of knowledge production; hone practical skills such as how to operate complex apparatuses, perform difficult experiments, and manage research groups; explore the frontiers of their disciplines; collaborate with world-class colleagues across fields; and develop professional networks that span the globe. All of this makes them better at what they do, a highly desirable outcome unless it prejudices US national security and economic interests or ethical and human rights norms.

To illustrate that point, US research institutions should welcome materials scientists and high-energy physicists from most foreign institutions and nations, but not those with active weapons research programs mobilized against US strategic interests. Likewise, collaborating with AI researchers or geneticists from countries with authoritarian surveillance states and weak human subjects protections is not equivalent to collaborating with those from democracies. Different standards and levels of scrutiny should apply. Context matters.

In principle, research institutions are best placed to make these decisions for themselves. But because their performance has fallen short of necessity, their credibility is increasingly at issue. Reclaiming it depends urgently on enhancing their internal controls in ways that are alive to the full spectrum of potential risks that their foreign engagements might entail and on developing processes and tools to make better decisions.

### *A. Think Strategically*

A comprehensive Global Engagement Risk Assessment & Management Program (GERAMP) would achieve those objectives. Such a program would rigorously assess the types and degrees of risk implicated in a

given venture and mitigate them to acceptable levels by suggesting proportionate governance and oversight strategies.

A GERAMP involves many considerations, but several are key. First, it should exercise *comprehensive oversight* over all of the institution's international engagements. Its associated policies and processes should foster cultures of integrity, safety, and security in order to protect the people, information, and assets that form the backbone of our academic and research ecosystems. Second, these policies and processes must be accompanied by regular *training in practical measures* to mitigate foreign engagement risk in informal and formal research activity; uphold core institutional values; protect affiliates and intellectual property; and support compliance with policies, laws and regulations.

Third, *transparent reporting* requirements are essential to effective risk management, as are processes that deliver reported information to decision makers in a timely and actionable manner and that archive this information for convenient, future reference. Policies governing conflicts of interest and commitment can catalyze that capacity by requiring prompt disclosures of external affiliations, relationships, and financial commitments. They have the added benefit of clarifying the responsibilities that affiliates have to their home institutions.

Fourth, when administrators perform a risk assessment, they should *document in detail* the information that they evaluated in order to guide not just future decisions but also re-examinations of past ones.

Fifth, institutions must incorporate into their risk reporting cycles *ongoing reviews* of their internal security strategies, policies, and processes, especially as these relate to foreign interference.

Implementing an effective GERAMP can play a major role in enhancing the security of an institution's personnel, facilities, and intellectual capital. For such a program to be effective, personnel must be aware of existing threats, be able to implement countermeasures when appropriate, and be observant of nontraditional collection activities directed at their institution. This is possible only if all members of the institution are cognizant of the range of threats to the research enterprise and actively support the risk assessment and management program.

# What Forms Can Countermeasures Take?

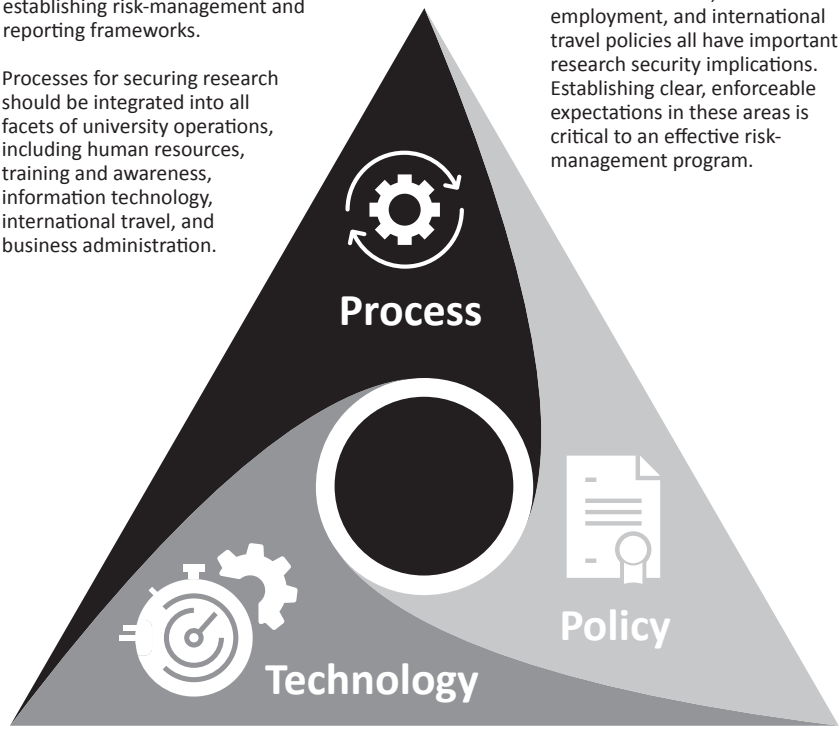
## Process Solutions

Process solutions include such actions as vetting visiting scholars, monitoring computer networks for illicit exfiltration of research data, incorporating data-loss prevention systems on networks, and establishing risk-management and reporting frameworks.

Processes for securing research should be integrated into all facets of university operations, including human resources, training and awareness, information technology, international travel, and business administration.

## Policy Solutions

Conflict of commitment, financial conflict of interest, external employment, and international travel policies all have important research security implications. Establishing clear, enforceable expectations in these areas is critical to an effective risk-management program.




## Technology Solutions

Incorporating technical solutions into your risk-management process, such as secure computing enclaves that meet federal requirements, can provide a solid foundation for securing data while minimizing the burden on researchers.

**Figure 1. A Structured Approach to the Problem.**

A GERAMP integrates mutually *reinforcing policy*, *process*, *and technology solutions* throughout a research institution's operations (Fig. 1). Key areas include: human resources, research and instruction, facilities security, information technology, international travel, development, and business administration.

To varying degrees, many research institutions already possess the elements of such a program.[15] But these frequently lack a strategic focus. The GERAMP confers conceptual and operational coherence upon them and brings them into alignment. It also establishes a methodology for identifying critical gaps and for ongoing optimization and growth.

It is beyond the scope of this chapter to supply an exhaustive list of such solutions, and institutional needs will vary. But for illustrative purposes, *clear policies* governing conflicts of commitment, financial conflicts of interest, external employment, international travel, and access to facilities and network resources are basic to effective risk management. Policies governing institutional accountability, the authority to contract, the duty of personnel to act in an institution's best interests, and the protection of dual-use technologies and controlled unclassified information (CUI) are valuable enhancements.

*Processes* are structured pathways through which policies are implemented. A GERAMP would, for example, establish processes to identify possible downstream applications of research undertaken in collaboration with foreign entities or research that might be a target for foreign interference or misappropriation. It would systematize the vetting of foreign entities across an institution, the monitoring of computer networks for unauthorized exfiltration of research data, and the implementation of data-loss prevention.

---

15. "University Actions to Address Concerns About Security Threats and Undue Foreign Government Influence on Campus," Association of Public & Land-Grant Universities, May 2020, https://www.aplu.org/members/councils/governmental-affairs/CGA-library/effective-science-and-security-practices---what-campuses-are-doing/file.

To those ends, research institutions could jointly establish and administer regional vetting centers staffed in part by cleared personnel authorized to enhance open-source vetting with insights drawn from sensitive or classified information. These regional centers would rationalize administrative spending, spread costs, and help to equalize the uneven distribution of actionable information, resources, and capacities across the research enterprise.

Regional vetting centers would be a platform through which member institutions could access expertise in critical languages and area knowledge. They would provide members access to open-source datasets for the purpose of conducting enhanced vetting of personnel seeking to access sensitive research. They would also be a ready source of advice and assistance in the vetting process.

In addition, regional vetting centers would provide centralized points of contact to liaise with the government on sensitive technologies, emerging threats, and new priorities in regulation and enforcement, as necessary. This would deepen mutual understanding and relationships of trust between government and research institutions, break down barriers to information sharing, and equip individual institutions to make better risk assessment and management decisions on their own terms.

The requirements to protect federally sponsored research have increased significantly over the past five years. Standards such as NIST Special Publication 800-171 Rev. 2 have imposed new regulatory burdens and financial costs on research institutions.[16] Incorporating *technological solutions* into the GERAMP can alleviate those hardships. For example, some institutions have established NIST 800-171-compliant Secure Computing Enclaves (SCEs) to house all of their federally funded research and to safeguard sensitive data.[17] These enclaves provide a

16. National Institute of Standards and Technology, U.S. Department of Commerce, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020, https://doi.org/10.6028/NIST.SP.800-171r2.

17. The Texas A&M University System Research Security Office Secure Computing Enclave, 2020, https://rso.tamus.edu/home/research-security/secure-computing-enclave.

preapproved secure infrastructure for internet connectivity, resource sharing, encryption, authentication schemes, and outside communications. They are physically separated from the institution's larger network yet operate transparently to minimize the burdens on their users.

Establishing SCEs at a regional level across the United States would allow member institutions to supply their research communities with security as a service at economies of scale. This would realize cost savings by reducing the need for institutions to duplicate one another's capital investments in compliant cyberinfrastructure. Member institutions would administer the enclaves jointly, with federal support for the purpose of strengthening the protection of the nation's most important research. Other technological solutions could also mitigate foreign engagement risk, such as the following:

- Robust access and device registration protocols that enforce minimum security standards and best practices on users of an institution's internal networks.
- Hardware encryption and high-performance VPNs to provide secure authentication and data protection on personally owned computing devices. This ensures that personnel are consistently using secure, managed computing platforms, even when they are working remotely or are outside of internal networks.
- Integrating commercial compliance management databases and private-sector threat management solutions into a research institution's due diligence program. These databases include products for management of export control processes, commercial sources for background checks, and more free-form databases that facilitate analysis of research relationships, collaboration, and sources of funding.

### *B. Establish a Global Engagement Review Office (GERO)*

Safely navigating foreign engagement risk begins with a strategic program backed by formidable investments in institutional capacities, such as mastery of pertinent regulatory regimes, knowledge of foreign languages, and

access to advanced subject matter expertise. But it also requires a stable, accountable authority with substantial institutional capital that can marshal those resources effectively across multiple constituencies.

A GERO could achieve that goal. In a typical university setting, this office would report and make recommendations directly to the provost and would serve as the institution's focal point for coordination and oversight of all matters related to foreign engagement. It would regularly convene and chair a body similar to an institutional review board that would include: the university's research security officer; authoritative representatives from the offices of the provost and vice presidents for research and international affairs, from the council of principal investigators, and from the office of general counsel; and, depending on the matters before it, relevant foreign area and subject matter experts and senior representatives from the institution's development, sponsored research, and government relations offices. More specifically, the office would exercise unified leadership over the following domains:

*1. Strategic Assessment and Management of Foreign Engagement Risk*

- Institute a Global Engagement Maturity Model (GEMM, discussed below) to formalize the implementation and optimization of the GERAMP.
- Supervise GERAMP implementation, monitoring, and enhancement in coordination with other stakeholders (e.g., information technology and human resources).
- Advise institutional leadership and stakeholders on foreign engagement risk in accordance with established policies and processes.

*2. Foreign Contracts, Gifts, and Compliance*

- Produce up-to-date, practical guides, checklists, and templates on the institutional policies and processes governing foreign research collaborations, contracts, grants, and gifts. These will help to mitigate many of the risks posed by foreign engagements, and promote fulfillment of disclosure and reporting requirements, particularly

with respect to conflicts of interest and commitment. Train and periodically refresh personnel on these resources.[18]

- Systematically review all substantive engagements with foreign entities, whether formal or informal, for risk. The scope of this review will depend on the identity of the foreign entity and the nature of the engagement. Most cases will exit the review process at an early stage, parts of which could be implemented using online screening tools. Some cases will require higher levels of scrutiny. Archive the inputs to each review and its findings for future reference.
- Offer in-house consulting services on foreign engagement risk to empower local personnel on their own initiative to safeguard core academic values, research integrity and security, legal compliance, and institutional interests.
- Systematize data collection, metrics, disclosures, and reporting to satisfy GERAMP monitoring and compliance mandates related to foreign engagements.

*3. Personnel*

- Train and embed global research integrity and security officers throughout the institution as first points of contact. Depending on caseload, this role may be one of several in an individual's job description, particularly at lower levels of the institution's structure.
- Systematically vet foreign entities such as visitors, students, scholars, research collaborators, and research sponsors commensurate with the risks that they pose. Regional vetting centers could pool resources and data inputs, uniformly raise standards, and provide common points of contact for information sharing with peer institutions and the government.

---

18. In 2019, the AAU and APLU recommended a comprehensive communication campaign to raise awareness of current reporting requirements among faculty and other members of university communities. This recommendation should be expanded to encompass information and research security. Association of Public & Land-Grant Universities, https://www.aplu.org/projects-and-initiatives/research-science-and-technology/science-and-security.

- Analyze insider threats and adopt safeguards. Any person with access to technology and intellectual capital could transfer it without proper authorization. Clear procedures and training can mitigate this hazard and promptly detect its occurrence.
- Institute processes to promote and verify full disclosure of foreign interests and commitments.
- Institute processes to promptly revoke access to institutional systems and resources for affiliates upon separation.

*4. Foreign Research Collaborations*

- Analyze the potential end uses of research, whether fundamental or not. Identify and protect sensitive data and technologies, especially those with dual-use applications or with externalities that impinge on health and safety, core values, and ethical or human rights concerns.
- Create robust disclosure requirements for intellectual capital, particularly when it has commercial potential, so that measures can be taken early to safeguard it, such as applying for patent protection.
- Implement research communication agreements. Intellectual capital loss or property theft by untrustworthy or malign members of research teams is a persistent occurrence. Adopting a research communication agreement can mitigate this threat. Research communication agreements are used extensively in government and the private sector. They help research teams internalize sound information security practices by outlining a team's communication protocol, establishing ethical obligations to keep research materials confidential, and defining processes for sharing and releasing data.

Protecting potentially sensitive research results is especially challenging because it can be difficult to know in advance if results will be sensitive or valuable. Government program managers cannot bear the burden of determining this alone. All stakeholders have a responsibility to protect sensitive or valuable information and ensure that it is handled securely. A research communication agreement represents a middle

ground, providing a baseline layer of security that the principal investigator can augment mid-stream if appropriate.

*5. Cyber*

- Train personnel on cyber threat abatement and require periodic refreshers. End users are the most common vectors for cyber threats, but training can thwart these. Tech savviness is no guarantee that an individual appreciates the intricacies associated with this class of threat or the degree to which the research community is targeted.
- Implement Secure Computing Enclaves. These shared environments will rationalize expenditures and ease the uptake of best security practices without impeding research.

*6. Foreign Travel*

- Adopt institutional duty of care policies to protect personnel overseas.
- Institute review processes for foreign travel with respect to export controls, shipping, software use restrictions, and other security and safety concerns.
- Train affiliates located or travelling overseas in context-specific risk management and mitigation practices. Offer political risk counseling and technological support services, such as hardening smartphones, tablets, laptops, and other electronic devices against cyberattacks, cleaning them after travel to countries that are known threats, or supplying loaner devices.

*7. Incident Reporting and Response*

- Institute internal processes for reporting, investigating, and documenting foreign interference and exploitation.
- Supervise responses to research integrity and security incidents involving foreign entities in accordance with established incident and investigation processes.
- Recommend disciplinary processes for compliance failures of omission and commission.

- Preside over consultations with intelligence and law enforcement agencies, as necessary.

*8. Sectoral Engagement*

- The Academic Security & Counter Exploitation (ASCE) program was established in 2017 to help address the threat posed by foreign adversaries to US academic institutions.[19] This group initially consisted of universities conducting classified research and focused on specific processes and controls to protect sensitive information. The group has since expanded both its membership and its focus to deal with broader policy issues related to foreign interference. As of mid-2020, the group has more than four hundred members from more than 150 colleges and universities.
- The Association of University Export Control Officers (AUECO) is composed of export control officers and other compliance officers at US institutions of higher education.[20] University export control officers are primarily responsible for compliance with export, import, and trade sanctions policies such as the Entity List, but are frequently involved in other aspects of foreign engagement risk. AUECO provides a forum for information exchange and collaboration among its members and analyzes and advocates for policies and regulations of interest to higher education.
- The Council on Government Relations (COGR) is an association of leading research universities, affiliated medical centers, and independent research institutes that focus on the conduct of research at the highest standards; informed decision making on issues critical to the research and higher education community; and on deriving maximum benefit from investments in research conducted at member institutions.[21] COGR is an authoritative source of information, analysis, advice, policy perspective, and historical context for its members in the areas of research administration and compliance, financial oversight, and intellectual property.

19. Academic Security & Counter Exploitation Program, https://asce.tamus.edu.
20. Association of University Export Control Officers, http://aueco.org.
21. Council on Government Relations, https://www.cogr.edu.

*9. Government Relations*

- It is in the mutual interest of research institutions and the government to establish relationships of trust that can facilitate concise and accurate information sharing, appropriate oversight of federally funded research, and the early identification and protection of sensitive research. Establishing a single point of operational accountability or contact with the government for foreign engagements simplifies these tasks and helps institutions to stay abreast of trends and changing guidelines, prepare for new requirements, and avoid surprises.

Finally, the GERO would complement and coordinate with units that commonly fall under the authority of the vice provost for research to:

- Enhance export control offices at institutions that have them and create such offices at institutions that don't.
- Improve compliance with export control and related regulatory requirements and ensure successful implementation of technical control plans.
- Fully integrate protective security in planning, selecting, designing, and modifying facilities for the protection of personnel, information, and physical assets.
- Establish physical security measures that minimize or remove the risk of: a) harm to people; b) information and physical assets being rendered inoperable or inaccessible, or accessed, used, or removed without authorization.

*C. Change the Paradigm*

A GERO could be the cornerstone of a more robust approach to managing the foreign engagement risks that research institutions increasingly face, but without a corresponding paradigm shift from compliance-driven formalism to proactive Operational Security (OPSEC), its full potential might never be realized. OPSEC supplies a workflow for sustaining vigilance and innovation. It originated with the US military and involves five iterative steps (Fig. 2).

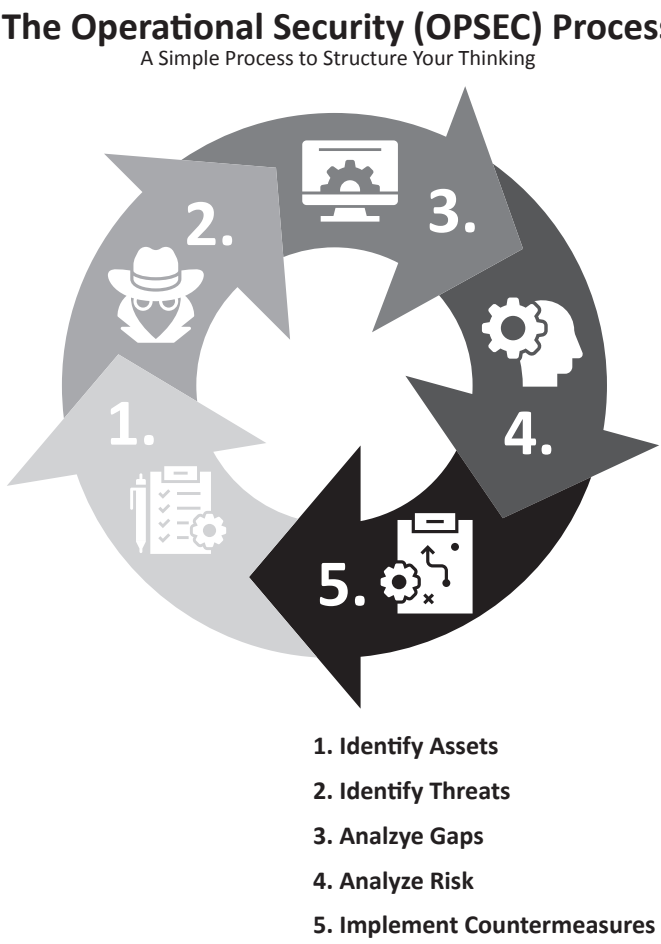



**Figure 2. The OPSEC Process.**

- *Identify assets.* This includes sensitive information such as research data, intellectual property, export control data, and personnel records.
- *Identify threats.* Evaluate the potential value of each category of sensitive information to third parties and institutional insiders and the threats that they may pose.
- *Analyze gaps.* Evaluate current safeguards, security gaps, and other vulnerabilities to determine what, if any, loopholes or weaknesses exist that could be exploited to gain access to sensitive information.

- *Analyze risk*. Compare threats and vulnerabilities to assess the potential risks posed by nontraditional collection activities and the likelihood of their occurrence. Nontraditional collection activities can occur during informal personal encounters over email, in labs, during conferences, and in other academic exchanges.
- *Implement countermeasures*. Formulate and execute a plan to reduce threats and mitigate risks. This might include updating hardware, creating new policies regarding sensitive information, or training affiliates on sound security policies and practices. Cost/benefit analysis can be used to evaluate potential countermeasures. Countermeasures should be straightforward, minimally invasive, and simple for affiliates to implement.

### *D. Create a Global Engagement Maturity Model*

If the GERO drives the execution of an institution's GERAMP, then the GEMM provides the *strategic roadmap* for shepherding that program from its inception to full integration with all aspects of the institution's operations. Leading the formulation and adoption of a GEMM that reflects the institution's circumstances, in collaboration with institutional leadership and key stakeholders, should be among the first duties of the GERO. This will require substantial investment and institutional capital but will create long-term value.

#### *1. What is Global Engagement Maturity Modeling?*

The GEMM provides a formal method for assessing the policies and processes in an institution's GERAMP and ensuring that they are effective, replicable, and continuously improved. Information technology provides one path for successfully automating and integrating those elements into the institution's overall operational infrastructure. Institutions adopt a GEMM with a graduated set of risk assessment and management levels defined by progressively more demanding ("mature") requirements (Fig. 3).

The GEMM is a variant of the capability maturity models (CMM) used extensively in the private sector, particularly in the software industry. Both the Department of Homeland Security and the National

# Global Engagement Maturity Model

The Research Security Capabilities Maturity Model provides an objective methodology for assessing an organization's overall security program maturity.

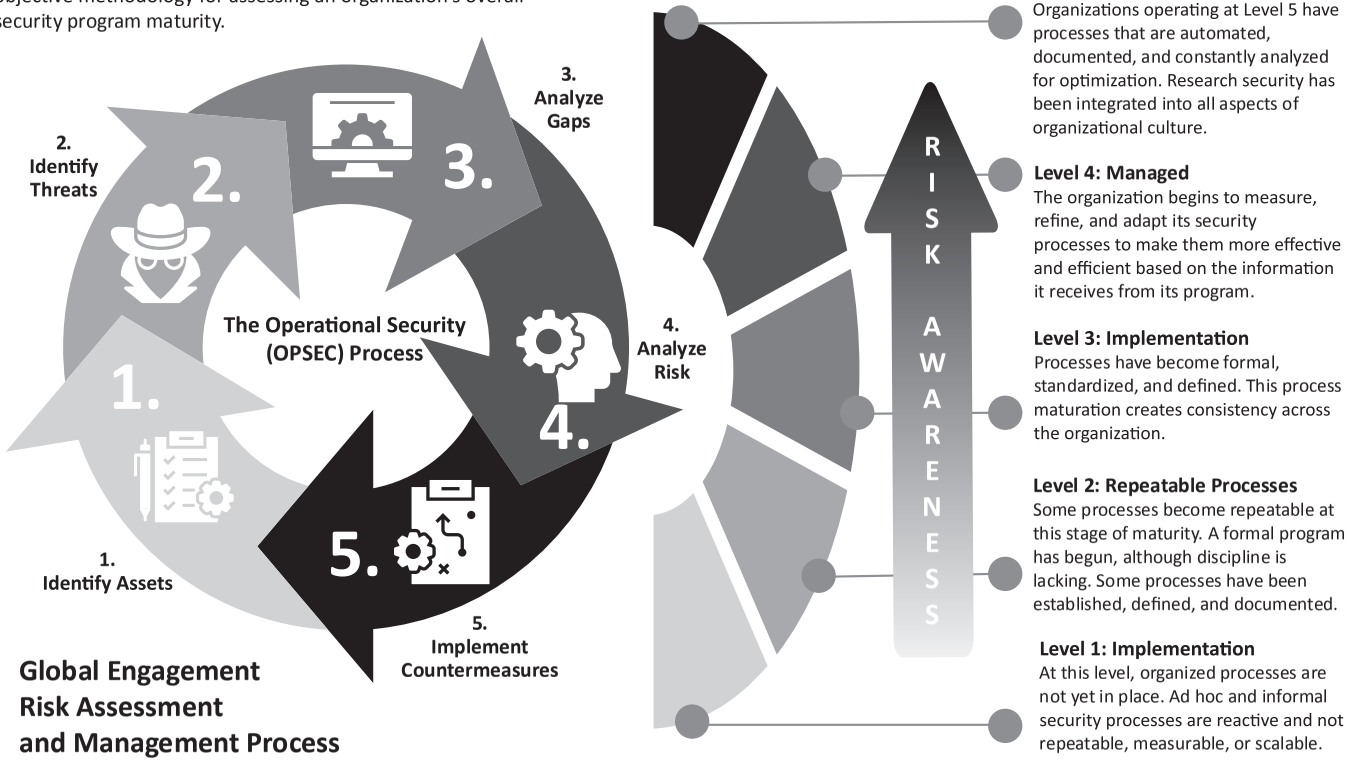



**Figure 3. Global Engagement Maturity Model.**

Institutes of Standards and Technology offer guidance on building and integrating CMMs.[22]

Adopting a GEMM offers several benefits. First, it promotes a shared vocabulary and conceptual understanding of foreign engagement risk assessment and management. Second, it lays out a roadmap with clear benchmarks for performance and improvement. Third, it helps an institution to identify and remediate vulnerabilities and areas that are reactive to security threats in order to achieve a stronger, proactive posture. Finally, a GEMM would communicate to funding agencies a grant-receiving institution's level of preparedness and the corresponding types of work that it can perform effectively and securely.

*2. What does a Global Engagement Maturity Model look like?*

A GEMM comprises five distinct maturity levels, each defined by a corresponding set of key process areas that, when implemented together, satisfy the goals defined for that level. As an institution advances from one maturity level to the next, its GERAMP will move from unorganized and unstructured to disciplined, structured, and continuously optimized. Policies supply the overarching guidance for the program and will evolve to support its maturing structure. Processes are the step-by-step methods that fulfill policy requirements and contribute to the program's success. They will evolve as the program achieves higher degrees of optimization.

***Level 1: Initial Policies***

Institutions enter this level with no standardized processes in place. They are ad hoc, informal, reactive and not repeatable, measurable, or scalable. This level of maturity is characterized by the following:

22. Department of Homeland Security, *Cybersecurity Capability Maturity Model White Paper*, May 2014, https://niccs.us-cert.gov/sites/default/files/Capability%20Maturity%20Model%20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf; National Institute for Standards and Technology, Information Technology Laboratory Computer Resource Security Center, June 22, 2020, https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels.

- Formal, up-to-date, documented policies that are readily available to employees and expressed as "shall" or "will" statements.
- Policies that establish a continuing cycle of risk assessment and implementation and employ monitoring for effectiveness and compliance.
- Policies covering specific assets or all major facilities and operations institution-wide.
- Policies that have been approved by key stakeholders.
- Policies that delineate the structure of the GERAMP, clearly assign GERO responsibilities, and lay the foundation necessary to reliably measure progress and compliance.
- Policies that identify specific penalties and disciplinary actions for non-compliance.

Institutions at Level 1 of the GEMM should focus on developing basic policies necessary to establish repeatable processes in preparation for advancement to GEMM Level 2.

***Level 2: Repeatable Processes***

At this level, a formal program has been initiated but discipline is lacking. Some processes have been established, defined, and documented and are repeatable. This level of maturity is characterized by the following:

- Formal, up-to-date, documented processes to implement the security controls identified in Level 1 policies.
- Processes to clarify where, how, when, and on what a control is to be applied and who is to apply it.
- Processes that document the implementation of and the rigor with which a control is to be applied.
- Processes that clearly define research security responsibilities and expected behaviors for: a) institutional leadership and administration; b) employees and affiliates (e.g., faculty, staff, and students); c) security administrators (e.g., IT, research security); d) processes that list appropriate individuals as points of contact for further information, guidance, reporting, and compliance.

Institutions at Level 2 of the GEMM should focus on developing standard processes through greater attention to documentation, standardization, and integration in preparation for advancement to GEMM Level 3.

***Level 3: Implementation***

At this level, processes are formalized, standardized, and defined. This promotes consistency across the institution. At this level of maturity:

- Processes are communicated to the individuals who must comply with them.
- Research security processes and controls are implemented in a consistent manner everywhere that they apply and are reinforced through training.
- Ad hoc, individual, or case-by-case approaches are discouraged.
- Policies are approved by key affected parties.
- Initial testing is performed to ensure controls are operating as intended.

Institutions at Level 3 of the GEMM should begin to focus on monitoring and controlling processes through data collection and analysis in preparation for advancement to GEMM Level 4.

***Level 4: Managed***

At this level, the institution begins to measure, refine, and adapt their GERAMP processes to make them more effective and efficient based on feedback generated by their program. At this level of maturity:

- Tests (including self-assessments performed by staff, contractors, or other designated parties) are conducted routinely to ensure that all policies, processes, and controls are performing as intended and that they meet the appropriate level of the GEMM.
- Information gleaned from records of potential and actual foreign interference and other related security incidents and from alerts, such as those issued by IT security administrators, qualify as test results. This information can identify specific vulnerabilities and provide insights into threats and risks.

- Independent audits, such as those arranged by funding agency Inspectors General, provide valuable feedback about an institution's performance but are not substitutes for routine and rigorous internal testing.
- Prompt and effective remediation is taken to address identified vulnerabilities.
- Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented.
- The frequency and rigor with which individual processes and controls are tested depend on the risks posed by them not operating effectively.

Institutions at Level 4 of the GEMM should begin to focus on constant optimization by monitoring feedback from current processes and by innovating to better meet specific needs in preparation for advancement to GEMM Level 5.

***Level 5: Integration***

At this level, an institution's processes are automated, documented, and constantly analyzed for optimization. Risk assessment and management are part of the overall culture. However, reaching this level does not mean that the institution's maturity has peaked. It means that it is monitoring, testing, and adapting its processes constantly to make them better. At this level of maturity:

- There is an active and effective institution-wide GERAMP.
- The GERAMP comprises consolidated practices that are integral to the institution's culture.
- Implementation of the GERAMP is second nature.
- Policies, processes, implementations, and tests are continually reviewed and optimized.
- Decision making is based on risk and mission impact.
- Security vulnerabilities are studied and managed.
- Evidence-based re-evaluations of threats are continually conducted and controls are adapted to evolving research security environments.

- Additional research security measures and opportunities for innovation are identified as needed.
- Costs and benefits of research security are measured as precisely as practicable.
- Status metrics for the GERO are established and met.

### *E. A New US Government-Sponsored Entity*

US research institutions have a long way to go before they regain the initiative in their management of foreign engagement risk, and they cannot do it alone.[23] Government support is essential but currently scoped too narrowly to assist with the classes of the threat that this report explores. The open and collaborative nature of the US research enterprise creates an exceptionally soft target space that in many instances makes recourse to clandestine foreign operations such as espionage unnecessary. In the lightly policed realms of fundamental and applied research, a universe of risk flourishes within the bounds of the law and therefore outside of the counterintelligence and law enforcement frames of reference conventionally used by the government.

In principle, the public nature of this risk should make it easier to recognize and abate. But in practice, foreign adversaries prey on the credulity and incapacity of their hosts. They obfuscate their identities; mask references to defense-related partnerships and research projects by using alternative, innocuous or vague English-language translations or by omitting them altogether from their English-language materials; and employ other means of concealment.[24] US research institutions generally lack the internal capabilities to detect and penetrate those

23. White House Office of Science and Technology Policy, *Enhancing the Security and Integrity of America's Research Enterprise*, June 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise-June-2020.pdf.
24. Robert Delaney, "US Ties Activities of Arrested Chinese Military Officer to Those by Defendant in Boston Case," *South China Morning Post*, June 25, 2020, https://www.scmp.com/news/china/military/article/3090497/us-ties-activities-arrested-chinese-military-officer-those?utm_source=copy_link&utm_medium=share_widget&utm_campaign=3090497.

cloaks although they may hide in plain sight. As the journalist and author John Pomfret has observed with respect to the PRC, "The Chinese language is the first layer of encryption."[25] Analogous claims could be made of other critical languages, such as Farsi and Arabic.

To overcome these impediments, we recommend the constitution of a government-sponsored entity devoted to research and analysis of foreign engagement risk in the US research enterprise. The structure and legal authority such an entity would operate under, especially as it relates to privacy law, are to be defined by the executive and legislative branches. Nevertheless, we suggest an interagency or hybrid form. The entity's mission will necessarily intersect with the portfolios of education, defense, intelligence, law enforcement, and research funding agencies but must transcend their individual perspectives, integrate their information streams, and provide an urgently needed, unified point of contact for the research enterprise.

The entity would interface directly with our proposed GEROs and regional vetting centers to establish mutually beneficial relationships of trust, promote proactive postures of integrity and security, and empower research institutions to exercise their discretion with greater wisdom. While the entity could supply classified information as needed to vetting personnel who have the appropriate clearances, by working predominantly in an open-source environment, it would facilitate information sharing and foster more collaborative dynamics between government and the research community than current counterintelligence and law enforcement-driven initiatives support. More specifically, the entity would:

- Establish a central office with regional satellites across the United States funded and administered by the government and staffed by area specialists, linguists, and officials experienced in identifying

25. John Pomfret, "What America Didn't Anticipate About China," *The Atlantic*, October 16, 2019, https://www.theatlantic.com/ideas/archive/2019/10/chinas-cultural-power/600049.

and mitigating foreign engagement risks to US research, especially with respect to technology transfer and the PRC.

- Fill protection gaps by focusing on entities and activities earlier in the R&D and technology lifecycles, which generally fall outside of regulatory oversight.
- Provide compliance and vetting support to federal agencies that fund the research enterprise and establish mechanisms for periodic monitoring to ensure continued compliance with federal grant and contracting requirements.
- Serve as a principal point of contact and conduit for GEROs and regional vetting centers to exchange information and obtain strategic threat assessments, tactical due diligence, and vetting support.
- Combine the research and analytic capabilities of the US government, think tanks, and academia to publish studies, assessments, and policy recommendations for clients in the research enterprise and government.
- Review open-source publications in key linguistic and geographic spaces to identify high-risk foreign engagements, especially those related to military R&D or emerging civilian technologies with potential dual-use or high-value commercial applications.
- Serve as an authoritative source to advise research institutions on emerging technologies important to national security.
- Collect and analyze information on all identifiable state-sponsored talent recruitment programs to determine the extent of their activity in the United States.
- Build databases derived from publicly available information on: entities that support the defense research and industrial base of strategic competitors, entities that are tied to foreign state-directed technology transfer missions and covert influence operations in the United States, and entities that support the surveillance and security apparatuses of states that engage in systematic human rights abuses. These databases could be designated controlled unclassified information.
- Create a model for other nations, help them to develop similar capabilities, and assemble coalitions.


**Figure 4. Thinking about Global Engagement.**

## V. Conclusion

The excellence of the US research enterprise is inseparable from its commitments to openness and academic independence, its institutional autonomy, and its discretion to operate in a globalized world. However, in a climate of sharpening strategic competition, these qualities also engender vulnerabilities that are increasingly prejudicial to national and economic security.

Evidence points to serious structural and conceptual flaws in the ways that research institutions and government each approach foreign engagement risk. Although incremental reforms may eke out better performance, the current system is decentralized and permissive by design and was never equipped to coherently navigate among the countless shades of gray that now beset it. Asked to fight a battle that it cannot win, its insufficiencies are corroding trust and exhausting patience among policymakers. The danger is that the remedies they ultimately devise may leave the research enterprise and the nation weaker and more isolated.

This chapter offers a way out of that breakdown (Fig. 4). It asks the research community and government to reinvent their approaches to foreign engagement risk so that they can meet one another in the middle, each bringing to the table what it does best. *First*, a research institution's GERAMP creates a strategic framework for rigorously assessing risk and mitigating it through proportionate governance. *Second*, its GERO operationalizes that framework, providing unified administrative leadership, oversight, and coordination across the institution. The GERO liaises with government directly and through joint regional vetting centers. *Third*, OPSEC primes institutions to use the GERO to reclaim the initiative by shifting from compliance-driven formalism to a proactive, adaptive posture. *Fourth*, the GEMM provides a structured methodology for continuous improvement. And *fifth*, a government-sponsored entity contributes its unique research and analytic capabilities to this apparatus and supplies a unified point of contact on foreign engagement risk.

The goals? To empower research institutions and scholars to pursue foreign engagements with the confidence that they can make better and

more granular decisions, to acknowledge and honestly grapple with the potential tensions between those engagements and national interests, and to deepen mutual respect and collaboration between the research enterprise and the government. All of this will admittedly require new investment, but much can be achieved by resolutely changing the paradigm to align and harness existing assets more effectively. It is imperative that we pull out of the trajectory that we are now on; the stakes are too high not to.