



# HOMELAND SECURITY ACADEMIC PARTNERSHIP COUNCIL


Foreign Malign Influence in  
Higher Education Subcommittee

Office of Partnership and Engagement  
June 3, 2024



Homeland  
Security

This publication is presented on behalf of the Homeland Security Academic Partnership Council (HSAPC) Foreign Malign Influence (FMI) in Higher Education Subcommittee, chaired by Dr. Miriam Feldblum and Dr. Antonio Flores, for the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.

 Digitally signed by Miriam Feldblum  
Date: 2024.06.03 18:11:05 -04'00'

---

Dr. Miriam Feldblum, Co-Chair  
Executive Director  
Presidents' Alliance on Higher  
Education and Immigration

**Antonio Flores** Digitally signed by Antonio Flores  
Date: 2024.06.04 09:14:33 -05'00'

---

Dr. Antonio Flores, Co-Chair  
President & CEO  
Hispanic Association of Colleges  
and Universities

This page is intentionally left blank.



<b>SUBCOMMITTEE MEMBERS .....</b>	<b>5</b>
<b>HSAPC STAFF .....</b>	<b>5</b>
<b>EXECUTIVE SUMMARY.....</b>	<b>6</b>
KEY FINDINGS: RESEARCH SECURITY.....	6
KEY FINDINGS: TRANSNATIONAL REPRESSION .....	7
RECOMMENDATIONS: RESEARCH SECURITY .....	7
RECOMMENDATIONS: TRANSNATIONAL REPRESSION .....	7
RECOMMENDATIONS: OVERARCHING.....	8
<b>METHODOLOGY.....</b>	<b>8</b>
<b>KEY FINDINGS.....</b>	<b>8</b>
RESEARCH SECURITY .....	9
TRANSNATIONAL REPRESSION.....	17
<b>RECOMMENDATIONS.....</b>	<b>21</b>
RESEARCH SECURITY .....	21
TRANSNATIONAL REPRESSION.....	22
OVERARCHING RECOMMENDATIONS.....	25
<b>CONCLUSION.....</b>	<b>26</b>
<b>APPENDIX 1: TASKING LETTER .....</b>	<b>27</b>
<b>APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES.....</b>	<b>29</b>

## SUBCOMMITTEE MEMBERS

<b>Dr. Miriam Feldblum</b>	Executive Director, Presidents' Alliance on Higher Education and Immigration
<b>Dr. Antonio R. Flores</b>	President and CEO, Hispanic Association of Colleges and Universities
<b>Dr. Farnam Jahanian</b>	President, Carnegie Mellon University
<b>Dr. Cynthia Kelley</b>	President and CEO, Madisonville Community College
<b>Dr. Tamarah Pfeiffer</b>	President, Southwestern Indian Polytechnic Institute
<b>Barbara Snyder</b>	President, Association of American Universities
<b>Meredith Asbury</b>	Assistant Vice President for Government Relations and Public Policy at the Association of American Universities
<b>Tricia O'Reilly</b>	Chief of Staff at Carnegie Mellon University
<b>Dr. Jay Parrent</b>	Vice President, Administration Madisonville Community College
<b>Dr. Eligio David Mendez Pagan</b>	Vice President and Chief of Staff, Hispanic Association of Colleges and Universities

## HSAPC STAFF

<b>Patrese Roberts</b>	Deputy Director
<b>Alexander Jacobs</b>	Senior Director, HSAPC Support
<b>Cori Dawson</b>	HSAPC Support
<b>Sofi Forwood</b>	HSAPC Support

## EXECUTIVE SUMMARY

On November 14, 2023, Secretary Mayorkas tasked the Homeland Security Academic Partnership Council (HSAPC) to form a subcommittee on foreign malign influence (FMI) in higher education to develop recommendations on guidelines and best practices for higher education institutions to reduce and counter FMI; to consider a public-private partnership to enhance collaboration and information sharing on FMI; and to assess how the U.S. Government (USG) can improve its internal operations and posture to effectively address FMI-related national security risks to higher education institutions.

To set the context for the Subcommittee, the Department of Homeland Security (DHS) reported that it has seen malign actors employ various tactics to achieve FMI, including:

- Monitoring, intimidating, and threatening students on U.S. campuses or targeting the overseas families of international students attending U.S. institutions to silence dissenting views;
- Persuading or pressuring academics to self-censor views they might oppose;
- Influencing publications they view as denigrating to their own interests or views;
- Funding research and academic programs, both overt and undisclosed, that promote their own favorable views or outcomes; and
- Stealing the resources, expertise, and products of academic research conducted at colleges and universities.

These actions undermine the trust and transparency essential to maintaining the integrity of our higher education system and support of students and scholars on our campuses. They jeopardize U.S. national security and the free exchange of ideas.

In preparation for this report, the Subcommittee received briefings from DHS subject matter experts, the Federal Bureau of Investigation (FBI), Department of State officials, the White House National Security Council (NSC), non-government organizations (NGOs), higher education associations, and senior campus officials from various research universities. During these briefings, members heard consistent themes, leading to key findings related to research security and transnational repression (TNR):

### KEY FINDINGS: RESEARCH SECURITY

- The federal government has taken numerous actions to address research security across federal agencies. Agencies have also taken steps to mitigate threats specific to their research environment and implemented several new policies enacted by Congress.
- Many universities have established effective practices to address research security on their campuses to reduce the risk of and counter FMI in the research environment.
- Existing forums and task forces can continue to bring together sectors of the USG (including DHS) and academia to coordinate and share resources on research security. More can and should be done to share timely case studies and actionable information with institutions.

- Previous enforcement actions, especially those resulting from the China Initiative and Presidential Proclamation 10043, have damaged trust between the USG and the academic research community.

#### **KEY FINDINGS: TRANSNATIONAL REPRESSION**

- TNR is an emerging issue that is still being fully understood, defined, and detected, and lacks concrete data and metrics.
- There are several government agencies and higher education associations being tasked with addressing TNR, but there is a lack of understanding on how these efforts will be linked or coordinated.
- Addressing TNR requires a nuanced, tailored approach. Enhanced transparency from government agencies, improved communication with campus leadership, comprehensive training, increased awareness, and clear points of contact are essential.
- The proliferation of online tools and platforms, including social media, facilitates the advancement and dissemination of TNR while complicating the tracking and identification of perpetrators. Targets often include individuals in diaspora communities and their family members in their home countries, contributing to the underreporting of TNR incidents.
- TNR incidents pose a serious threat to the academic freedom and freedom of expression of targeted students and scholars. Consequently, these issues should be of concern to educational and research institutions.

To address these findings, the Subcommittee makes the following three research security recommendations, four TNR recommendations, and two overarching recommendations to DHS:

#### **RECOMMENDATIONS: RESEARCH SECURITY**

1. Inform universities of the threat landscape, trends, and update research security case studies.
2. Coordinate with other agencies on research security issues and utilize existing programs to engage universities.
3. Engage with university and Asian-American groups to limit inadvertent harm of policies or enforcement actions on academic researchers and consider staff training opportunities.

#### **RECOMMENDATIONS: TRANSNATIONAL REPRESSION**

1. Develop a whole-of-government strategy to respond to incidents of TNR.
2. Compile resources and effective practices that help facilitate awareness-building and identify training opportunities.
3. Designate agency and university points of contact and TNR reporting mechanisms to ensure two-way communication between the FBI, DHS, other agencies, and university administrations.

4. Institute timely data sharing so we can move beyond anecdotal reporting and develop better tools to quantify instances of TNR on campuses and inform subsequent actions taken.

## RECOMMENDATIONS: OVERARCHING

1. Look to the past to inform the future. The evolution of coordination between higher education and government agencies can provide lessons to inform a framework for a measured, transparent, and consistent approach for both research security and protection from transnational repression.
2. Continue to invest in strengthening research and education institutions, which are the bedrock of our national security, and support the recruitment and retention of top talent to ensure U.S. competitiveness.

## METHODOLOGY

The Subcommittee began their research with briefings from DHS offices and components, including the Office of Intelligence and Analysis (I&A), the Office of Partnership and Engagement (OPE), Homeland Security Investigations (HSI), and the Office of State and Local Law Enforcement (OSLLE). The Subcommittee also received briefings from the FBI and the U.S. Department of State (DOS).

After gaining a deeper understanding of the law enforcement perspective, the Subcommittee met with subject matter experts from the U.S. National Science Foundation (NSF), an NGO leading the charge against TNR, Freedom House, and the Asian American Scholars Forum (AASF).

To round out their research, the Subcommittee held multiple roundtables with campus leaders and NAFSA: Association of International Educators who shared their experiences and best practices for addressing the issues of FMI and TNR. Further, the Subcommittee reviewed several key reports and resources.

## KEY FINDINGS

This report treats the broad umbrella of FMI as having two key spokes that connect us to our tasking and warrant individual examination.

The first area is research security, which emerged as an area of concern for the federal government and higher education institutions in 2018. Research security “involves the actions that protect our research communities from actors and behaviors that pose economic, strategic, and/or national and international security risks”<sup>1</sup> primarily in the

---

<sup>1</sup> G7 Working Group on Security and Integrity of Global Research Ecosystem, “G7 Common Values and Principles on Research Security and Research Integrity,” June 2022. Last accessed May 23, 2024, [https://www.bmbf.de/SharedDocs/Downloads/de/2022/220812-g7-sigre-paper.pdf?\\_\\_blob=publicationFile&v=2](https://www.bmbf.de/SharedDocs/Downloads/de/2022/220812-g7-sigre-paper.pdf?__blob=publicationFile&v=2).



context of fundamental research which is openly published and distinct from classified research in which most universities do not engage. The combination of advanced technology, human talent, and a democratic society has made the U.S. an attractive target for malign foreign actors seeking to access key ingredients for dominating the global innovation market. In this context, national security and research agencies are taking a renewed interest in protecting and securing federally funded research in the face of rising geopolitical concerns. Likewise, universities are seeking clear guidance from the federal government on how to best address foreign engagements without infringing on academic freedom or unduly targeting foreign scholars.

The second area is transnational repression, and while we note the lack of a consistent definition as one of our key findings, the term “transnational repression” or “TNR” refers to the practice by which authoritarian regimes target individuals or groups beyond their borders, often through extrajudicial means, to suppress dissent, silence opposition, or punish perceived threats to their power. This can include harassment, intimidation, surveillance, abduction, or even assassination of dissidents or critics living abroad. This is a developing national security concern that universities should have awareness of when seeking to welcome and support international students and scholars.

There may be instances when FMI can manifest itself in ways that defy or bridge these two categories, including visa exploitation, disinformation and misinformation campaigns, and foreign investment into critical infrastructure.

- **Visa exploitation:** When nation state actors are engaging in non-traditional collection in which non-citizen students conducting research in the U.S. are working to unlawfully acquire sensitive technology or access to research. This violates the terms of their visa.
- **Disinformation and misinformation campaigns:** The use of social media to spread disinformation and misinformation to the U.S. public for the purposes of continuing foreign objectives.
- **Foreign investment into critical infrastructure:** Interest in or acquisition of land geographically situated near federal government facilities or research laboratories.

## RESEARCH SECURITY

**The federal government has taken numerous actions to address research security across federal agencies. Federal agencies have also taken steps to mitigate threats specific to their research environment and implemented several new policies enacted by Congress.**

Initial concerns about FMI, later defined as research security, became evident after several high-profile cases were brought to the FBI in 2018. The government alleged that some academic researchers at U.S. universities hid certain foreign affiliations, failed to disclose information to research funding agencies, and committed wire fraud, tax fraud, and/or visa fraud. The Subcommittee heard from several briefers about the tremendous amount of work that has been done across the federal government and at universities to address this issue, especially in the last six years.

In response to threats of FMI in the federal research enterprise, in 2021, the Trump Administration released National Security Presidential Memorandum 33 (NSPM-33),<sup>2</sup> which established policy on how the federal government should address research security concerns. This was followed in 2022 by the Biden Administration's release of implementation guidance for NSPM-33, which outlined several areas the federal government should establish consistent policies and procedures to address research security.<sup>3</sup> Consistent with NSPM-33 and the implementation guidance, in 2024, the White House Office of Science and Technology Policy (OSTP) released guidance to federal agencies on implementing the common disclosure forms which standardize information collection and require federal research applicants to provide more information on their foreign affiliations, including on connections to foreign talent programs.<sup>4</sup> Additional guidance from OSTP outlining the research security program requirements for institutions of higher education is also anticipated.

In addition to cross-agency policies, several agencies have taken steps to mitigate threats specific to their agency's work and are also implementing several new measures passed by Congress.<sup>5</sup> Since 2018, Congress has enacted over 20 new requirements, primarily through the annual consideration of the National Defense Authorization Act, as well as the CHIPS and Science Act of 2022 (P.L. 117-167), to address risk-based security reviews for U.S. Department of Defense (DOD)-funded research projects, faculty disclosures, malign foreign talent programs, research security training for faculty and staff, foreign gifts from countries/entities of concern, and Confucius Institutes. These policies have mostly set forth implementation at DOD and NSF.

In 2023, DOD announced a policy requiring all fundamental research projects selected for award to go through a review for potential conflicts of interest and conflicts of commitment arising from foreign influence.<sup>6</sup> Several briefers expressed appreciation for the transparency

---

<sup>2</sup> "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," January 14, 2021. Last accessed May 23, 2024, <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>.

<sup>3</sup> National Science and Technology Council Subcommittee on Research Security Joint Committee on the Research Environment, "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development," January 2022. Last accessed May 23, 2024, <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>.

<sup>4</sup> Arati Prabhakar, "Policy Regarding Use of Common Disclosure Forms for the 'Biographical Sketch' and the 'Current and Pending (Other) Support' Sections of Applications by Federal Research Funding Agencies," February 14, 2024. Last accessed May 23, 2024, <https://www.whitehouse.gov/wp-content/uploads/2024/02/OSTP-Common-Disclosure-Form-Policy.pdf>.

<sup>5</sup> Association of American Universities, "Actions Taken to Address Foreign Security Threats, Undue Foreign Interference, and Protect Research Integrity at U.S. Universities," January 3, 2024. Last accessed May 23, 2024, <https://www.aau.edu/key-issues/university-and-federal-actions-taken-address-research-security-issues>.

<sup>6</sup> U.S. Department of Defense, "Department of Defense Strengthening Efforts to Counter Unwanted Foreign Influence on DOD-Funded Research at Institutions of Higher Education," June 30, 2023. Last accessed May 23, 2024, <https://www.defense.gov/News/Releases/Release/Article/3445601/department-of-defense-strengthening-efforts-to-counter-unwanted-foreign-influen/>.

the DOD policy provides; the policy clearly outlines the risk mitigation process and manages expectations of academic institutions and researchers.

The NSF is currently implementing several policies and actions as mandated by the CHIPS and Science Act of 2022. The Foundation has developed training modules that meet the research security training requirement for all covered personnel and federal awards.<sup>7</sup> NSF is also taking steps to establish the SECURE Center, which will “empower the research community to make security-informed decisions about research security concerns” and provide information, tools, and services for institutions of all sizes to employ.<sup>8</sup> The SECURE Center will also provide opportunities for collaboration between institutions of higher education and the USG. Additionally, in March 2024, the JASON science advisory group released a report on “Safeguarding the Research Enterprise,”<sup>9</sup> which will inform NSF’s efforts to develop a risk mitigation process. Several briefers also noted their appreciation that NSF has engaged universities and the Asian American community in advance of implementation of several measures. This has helped establish trust between academic institutions, faculty, and NSF leaders.

Within the State Department, the two focal points on research security have been enhancing screening of visa applicants and engaging international partners on the U.S. approach to research security. Presidential Proclamation 10043 (PP10043),<sup>10</sup> which restricts F and J visas to certain graduate and post-graduate researchers from institutions that support the People’s Republic of China (PRC)’s “military civil fusion strategy,”<sup>11</sup> has been implemented to raise additional factors during the visa review process. This review is done prior to additional vetting measures.

Officials say screening measures resulting from PP10043 have had a “narrow” impact on visa denials, however, the lack of transparency about the visa refusals issued has made it difficult to understand if it has been effective in addressing the perceived problem. The lack of communication with campuses about the basis of visa refusals, including reentry refusals that impact students and scholars, adds to the concerns. On engaging international partners, the State Department has participated and held several convenings, including with G7 partners, to discuss research security. The Security and Integrity of the Global Research

---

<sup>7</sup> U.S. National Science Foundation, “Research Security Training.” Last accessed May 23, 2024, <https://new.nsf.gov/research-security/training>.

<sup>8</sup> U.S. National Science Foundation, “NSF 23-613: Research Security and Integrity Information Sharing Analysis Organization (RSI-ISA0),” August 2, 2023. Last accessed May 23, 2024, <https://new.nsf.gov/funding/opportunities/research-security-integrity-information-sharing/nsf23-613/solicitation>.

<sup>9</sup> U.S. National Science Foundation, “NSF announcement on JASON report: Safeguarding the Research Enterprise,” March 21, 2024. Last accessed May 23, 2024, <https://new.nsf.gov/news/nsf-announcement-jason-report-safeguarding>.

<sup>10</sup> Executive Office of the President, “Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China.” 85 FR 34353. June 4, 2020. Last accessed May 23, 2024, <https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic>.

<sup>11</sup> U.S. Department of State, “Military-Civil Fusion and the People's Republic of China.” Last accessed May 23, 2024. <https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf>.

Ecosystem's Working Group convened by the G7 countries has published common values, principles, and best practices on research security.<sup>12</sup>

Early on, the FBI and other enforcement agencies helped to elevate awareness of the threats and nefarious actions of malign foreign actors in the academic research context. Beginning in 2018 and 2019, the FBI, in close partnership with several higher education associations, convened two national academia summits<sup>13</sup> and several regional meetings. The FBI has also created an academic liaison program which has established contacts within the FBI field offices for institutions that receive training on the academic research environment. Many institutions and government officials have pointed to these relationship building efforts as an example of effective collaboration between government and universities.

Within DHS, HSI, which is the principal investigative arm of the Department, has been tracking instances of foreign entities utilizing higher education as collection platforms for intelligence gathering activities in the U.S. Subcommittee members observe that some of the examples shared during their briefings allege significant wrongdoing and instances of visa fraud, but there was no evidence that they constituted a significant number of cases. Briefers acknowledged the lack of data and their inability to estimate the scope of the problem. Project Shield America<sup>14</sup> and Project Campus Sentinel<sup>15</sup> may provide opportunities for DHS to promote briefings with institutions of higher education and provide more transparent data on trends and red flag indicators regarding FMI.

**Many universities have established effective practices to address research security on their campuses to reduce the risk of and counter FMI in the research environment.**

In 2018, FBI Director Christopher Wray testified at a hearing before the Senate Intelligence Committee that China was “exploiting the very open research and development environment we have”<sup>16</sup> and that universities were perhaps naïve to the threat this may pose. Considering that call to action, universities have responded to risks identified by the USG specifically related to research and collaborations with malign foreign entities and relationships with the PRC. Several briefers informed the Subcommittee this has led to institutions increasing their staffing and resources to address research security concerns. One senior research officer shared that they now spend over 50 percent more of their time devoted to research security issues on campus, compared to before 2018. Operating in this

---

<sup>12</sup> G7 Security and Integrity of the Global Research Ecosystem Working Group, “G7 Best Practices for Secure & Open Research,” May 2023.

[https://www8.cao.go.jp/cstp/kokusaiteki/g7\\_2023/2023\\_bestpracticepaper.pdf](https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/2023_bestpracticepaper.pdf).

<sup>13</sup> Federal Bureau of Investigation, “2019 FBI Academia Summit,” October 10, 2019. Last accessed May 23, 2024, <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2019-FBI-OPS-Academic-Summit-Summary.pdf>.

<sup>14</sup> U.S. Immigrations and Customs Enforcement, “Project Shield America,” last updated May 8, 2024. Last accessed May 23, 2024, <https://www.ice.gov/outreach-programs/project-shield-america>.

<sup>15</sup> U.S. Immigrations and Customs Enforcement, “Project Campus Sentinel,” last updated May 8, 2024. Last accessed May 23, 2024, <https://www.ice.gov/outreach-programs/campus-sentinel>.

<sup>16</sup> U.S. Government Publishing Office, “Hearing Before the Senate Committee on Intelligence of the United States Senate One Hundred Fifteenth Congress Second Session”, Page 50, February 13, 2018.

evolving threat context has led to institutions re-examining existing research collaborations, considering the potential risks to new research collaborations, informing faculty of regulatory changes and new disclosure policies, and implementing new reporting and mitigation strategies. As a result of increasing federal requirements, additional administrative burdens have been imposed on research faculty and staff, as well as added financial costs to institutions to meet compliance requirements.

In 2019 and 2020, the Association of American Universities (AAU) and the Association of Public and Land-grant Universities (APLU) identified and shared effective practices universities are employing to address concerns about research security threats and undue foreign influence on campus.<sup>17</sup> One of the effective practices includes establishing campus-wide working groups and task forces on research security which meet regularly to review the latest threats and response and discuss policy implementation. One briefer noted they have created three different working groups at their institution related to research security.

Universities have created centralized websites on current federal disclosure requirements and international travel policies. They are in the process of implementing new campus-specific training requirements and utilizing NSF's new training modules, both of which provide a baseline understanding of research security concerns across the research enterprise. Institutions have revisited several policies on disclosure of conflicts of interest, conflicts of commitment, international visitors on campus, export controls, and cybersecurity measures.

An area that has seen significant attention and progress from both federal research agencies and universities has been enhancing disclosure policies to more explicitly account for relationships with foreign entities and affiliations with foreign talent recruitment programs. As a result of the NSPM-33 implementation, which now requires standard common disclosure forms to be used across federal research agencies, universities have also reviewed their conflict-of-interest and conflict-of-commitment policies and made updates to faculty disclosure policies to more clearly identify foreign affiliations, relationships, and financial interests. This harmonization across federal research agencies has helped reduce the compliance burden for universities. However, further attention is needed to harmonize other areas that have added compliance burdens for universities related to research security.

One area of continuing evaluation for institutions is how to effectively mitigate risk. In broad terms, briefers informed the Subcommittee that efforts to mitigate risk — both by the government and institutions — must avoid usage of a one-size-fits-all approach and elevate awareness on how to discern high versus low risk. What this means for each institution is that they must consider what mitigation efforts best serve their own campus environment, based on their research portfolio, campus size, and campus structure. One example of how

---

<sup>17</sup> Association of American Universities, "University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus," May 2020. Last accessed May 23, 2024, <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf>.

institutions are approaching risk is demonstrated by the Massachusetts Institute of Technology (MIT) in their report on “University Engagement with China: An MIT Approach”<sup>18</sup> which outlines specific guidance for MIT research faculty, students, and administrators, as well as a centralized process for review of engagements with elevated risk.

Related to effective practices, several briefers expressed optimism that the SECURE Center, which NSF is working to stand up, will eventually be an effective mechanism to help disseminate guidelines and additional best practices across institution types. The SECURE Center will provide analysis on patterns of risk, frameworks, and information that will help institutions make informed decisions. This will also have tremendous benefits for institutions that are not as heavily focused on research and may not have the staff or resources to address key research security issues on their own.

**Existing forums and task forces can continue to bring together sectors of the USG (including DHS) and academia to coordinate and share resources on research security. More can be done to share timely case studies and actionable information with institutions.**

One of the primary coordinating mechanisms on research security for USG agencies has been the Research Security Subcommittee convened by the National Science and Technology Council (NSTC) and OSTP. Participating agencies include research funding agencies like NSF, DOD, National Institutes of Health, and the U.S. Department of Energy, as well as intelligence and enforcement agencies like the FBI, DHS, and the U.S. Department of Justice (DOJ). The Research Security Subcommittee has led the interagency implementation of NSPM-33, including development of the common disclosure forms and draft guidance on research security program standard requirements.

Subcommittee members recognize that the Research Security Subcommittee has been an effective forum in harmonizing policies across the government and would encourage the NSTC group to continue its interagency coordination efforts on NSPM-33 implementation, which has cross-cutting impacts on the federal research enterprise. At a time when research security regulations have substantially increased over the last several years, harmonized policies across agencies help to reduce the compliance burden for institutions and provide clear, consistent guidelines for all researchers to follow.

The National Counterintelligence Task Force (NCITF), led by the FBI, was established in 2019 to create a “whole-of-government approach to counterintelligence” and coordinate multi-agency counterintelligence operations. The NCITF helps establish common goals and strategy, threat prioritization, training, analytic support, technical expertise, coordination, standardization, and information sharing among various government agencies with counterintelligence operations.

The Subcommittee recognizes the importance of the Task Force in coordination of operations, especially on issues and threats that continue to evolve related to foreign

---

<sup>18</sup> MIT China Strategy Group, “University Engagement with China: An MIT Approach”, Cambridge, MA: Massachusetts Institute of Technology, November 2022. Last accessed May 23, 2024, <https://global.mit.edu/about/report-by-the-mit-china-strategy-group/>.

influence which are also not contained to one agency. In addition to the NCITF, the National Counterintelligence and Security Center (NCSC) has partnered with multiple federal agencies to develop a toolkit on “Safeguarding Science”<sup>19</sup> which provides curated resources to support best practices in protecting research and innovation. The toolkit remains a dynamic resource for government and non-government partners and provides opportunity for additional resources to be publicized to a broad stakeholder audience.

As concerns on research security began to emerge in 2018, there were limited forums for universities and the USG to engage. For example, the National Security Higher Education Advisory Board (NSHEAB), which was established in 2005, had been disbanded and left the higher education community with no direct forum to engage on emerging national security concerns.<sup>20</sup> These concerns led to the creation of the academic liaison program at the FBI and culminated in several convenings of higher education and national security leaders at two national summits and several subsequent regional meetings to discuss concerns about research security, establish effective practices, and bring together those across government and universities who work on these issues.

The FBI academic liaison program also designated points of contact in each of the FBI’s regional field offices who work on issues related to academia. This has strengthened coordination between the FBI and universities and promoted the sharing of information on emerging threats and concerns. Several briefers note this has been an effective coordinating mechanism and could also be a model for engagement elsewhere. The emergence of forums where government and universities have engaged on research security demonstrates that the sooner higher education institutions can be brought to the table on an issue, the more effective and efficient coordination can be to address a common challenge.

As part of the government-university coordination on research security, early engagement highlighted the need for concrete examples and case studies that could succinctly demonstrate the threat to institutions and provide enough detail to allow university leaders to take action to mitigate concerns in their research environments. It was evident throughout the Subcommittee’s briefings that a gap remains between anecdotal information shared by the USG and what universities can do with the provided information to mitigate future issues.

As the threat landscape continues to evolve and the USG and institutions together identify and address gaps in policy implementation, the Subcommittee is encouraged by the planned work for the SECURE Center, which will likely fill a vital role in synthesizing anecdotes and identifying patterns of risk that academic leadership can then use to inform decision making on their campuses. Additionally, the SECURE Center could provide a

---

<sup>19</sup> National Counterintelligence and Security Center, “Safeguarding Science.” Last accessed May 23, 2024, <https://www.dni.gov/index.php/safeguarding-science>.

<sup>20</sup> American Council on Education, “ACE, Higher Education Groups Express Concerns Over Elimination of FBI Higher Education Board,” April 30, 2018. Last accessed May 23, 2024, <https://www.acenet.edu/News-Room/Pages/ACE-Higher-Education-Groups-Express-Concerns-Over-Elimination-of-FBI-Higher-Education-Board.aspx>.

valuable forum that brings together university and government leaders to discuss emerging research security issues.

**Previous enforcement actions, especially those resulting from the China Initiative and Presidential Proclamation 10043, have damaged trust between the USG and the academic research community.**

Under the previous administration, the China Initiative launched in November 2018 and subsequently brought several cases involving academic researchers, although very few resulted in convictions. The Initiative ended in 2022, however the increased scrutiny and perceived bias against Asian-Americans has had a chilling effect on the research community. According to a national survey of over 1,300 Chinese American faculty, 72 percent feel unsafe in the U.S. and 42 percent are fearful of conducting research.<sup>21</sup>

The Subcommittee heard from several briefers who shared stories of faculty self-censoring their activities and no longer pursuing collaborations for fear of retribution, being afraid of collaborating with Chinese individuals, and even walking away from funding opportunities altogether for fear of being targeted down the line. As one brifer shared, “It’s not always clear what expectations and consequences may be regarding an enforcement action.”

In addition to the China Initiative, in May 2020, President Trump issued Presidential Proclamation (PP) 10043. The Biden Administration has maintained enforcement of this policy, which seeks to prevent visas from being given to any graduate students or researchers with certain ties to entities that support or implement the PRC’s military civil fusion strategy. State Department officials indicate the impact of PP10043 has been “narrow,” though the only public data to demonstrate this is not specific to graduate student denials, which is the focus of the proclamation.

The enforcement of PP10043 also raised concerns from some briefers about what connections are acceptable and when a graduate student or researcher’s affiliations would make their entry impermissible. Recent reports of Chinese students attempting to re-enter the U.S. and being turned back to China at U.S. ports of entry have compounded this fear and raised additional anxiety for those traveling outside the U.S. for academic conferences or to visit family around not knowing if they will be permitted to re-enter.

This reality has made it difficult for Asian American faculty to trust law enforcement, as they feel unnecessarily targeted. Law enforcement agencies like the FBI and DHS could do more to build trust with this community and work with organizations like the AASF to ensure enforcement policies do not inadvertently target or discriminate against people on the basis of race, ethnicity, and country of origin.

---

<sup>21</sup> Asian American Scholar Forum, “New Report Showcases Climate of Fear Among Asian-Origin Scientists and Researchers,” September 23, 2022. Last accessed May 23, 2024, <https://www.aasforum.org/2022/09/23/new-report-showcases-climate-of-fear-among-asian-origin-scientists-and-researchers/>.



## TRANSNATIONAL REPRESSION

**Transnational repression is an emerging issue that is still being fully understood, defined, and detected, and lacks concrete data and metrics.**

While it is beyond the scope of this Subcommittee to draft authoritative definitions, it became clear that the term “transnational repression” (also referred to as “TNR”) is not a broadly understood term, nor one that has a consistent definition. Several briefers acknowledged that TNR has no formal definition but mentioned that there are currently efforts underway in both the agencies and Congress to define it.

In a few briefings, questions arose around the importance of either more precise or more general language. As we consider gaining awareness on college and university campuses, “transnational repression,” or “TNR,” may not be the most effective language to promote awareness on campus. The shorthand of “TNR” also has high potential for being misinterpreted and does not center the need to support the potential targets of such actions. An alternative framing of “transnational protection” is more likely to elicit trust among impacted students and scholars. Other countries have adopted other terms, such as Australia’s use of “community interference.”

While the definition is under debate, there are, however, dedicated efforts to examine and diagnose TNR that are worth highlighting. For example, the Subcommittee engaged in a briefing with Freedom House, which monitors the state of freedom and democracy around the world and is currently engaged in a multi-year study of TNR. In 2021, Freedom House released the first comprehensive global survey of transnational repression, “Out of Sight, Not Out of Reach,” and has released several follow-up reports.<sup>22</sup> Their most recent report, “Addressing Transnational Repression on Campuses in the United States,” indicated that 3.5 million people globally are at immediate risk of being targeted by governments engaging in TNR activities. Additionally, between 2014 and 2022, Freedom House documented 854 incidents of TNR tactics by 38 governments in 91 countries.

Freedom House has benefitted from close collaboration with the FBI to identify foreign governments which may seek to harass, intimidate, or stalk certain individuals outside their home country to exert influence. For example, these individuals may be told that family members in their home country will be harmed. While there are currently 31 different

---

<sup>22</sup> Yana Gorokhovskaia and Isabel Linzer, *Defending Democracy in Exile: Policy Responses to Transnational Repression* (Washington, DC: Freedom House, June 2022). Last accessed May 23, 2024, [https://freedomhouse.org/sites/default/files/2022-05/Complete\\_TransnationalRepressionReport2022\\_NEW\\_0.pdf](https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf). Yana Gorokhovskaia, Nate Schenkkan, Grady Vaughan, *Still Not Safe: Transnational Repression in 2022*, (Washington, DC: Freedom House, April 2023). Last accessed May 23, 2024, [https://freedomhouse.org/sites/default/files/2023-04/FH\\_TransnationalRepression2023\\_0.pdf](https://freedomhouse.org/sites/default/files/2023-04/FH_TransnationalRepression2023_0.pdf). Jessica White, Grady Vaughan, and Yana Gorokhovskaia, *A Light That Cannot Be Extinguished: Exiled Journalism and Transnational Repression* (Washington, DC: Freedom House, December 2023). Last accessed May 23, 2024, [https://freedomhouse.org/sites/default/files/2023-12/TNR\\_Journalism\\_Report\\_12.2023\\_Digital.pdf](https://freedomhouse.org/sites/default/files/2023-12/TNR_Journalism_Report_12.2023_Digital.pdf). Yana Gorokhovskaia and Grady Vaughan, *Addressing Transnational Repression on Campuses in the United States* (Washington, DC: Freedom House, January 2024). Last accessed May 23, 2024, [https://freedomhouse.org/sites/default/files/2024-02/TNR\\_UniversityReport\\_2024F.pdf](https://freedomhouse.org/sites/default/files/2024-02/TNR_UniversityReport_2024F.pdf).

federal crimes related to TNR that an individual can be charged with in the U.S. per the DOJ, so far, it has been difficult to create a statute that encompasses all of those crimes.

Despite these and other important efforts, we found that there is a lack of clear evidence, data, or awareness about TNR incidents, their scope, or their frequency. Much of the discussion on TNR and its impact is based on anecdotal evidence; it is hard to extrapolate the scale to which such incidences are occurring. The reports and briefers acknowledge that fear of retaliation prevents many victims of TNR from reporting it to anyone.

As explained by briefers, international students and scholars who may be most at risk or experiencing the possibility of threats or coercion from their home countries may consider these threats as “the cost of studying or researching” in the U.S. Those individuals most directly impacted by threats of TNR may not see that they have any recourse for relief and therefore do not report concerning behaviors. Without greater awareness and understanding of these threats, most colleges and universities are not proactively educating their faculty, staff, and students about these trends and how to detect and address such behaviors.

**There are several government agencies and higher education associations being tasked with addressing TNR, but there is a lack of understanding on how these efforts will be linked or coordinated.**

As referenced above in relation to research security, we learned of several committees and working groups that have been tasked with examining and making recommendations on foreign malign influence and TNR. While the attention to this emergent area is laudable, it is unclear where the convening authority on this issue lies and how a whole-of-government approach can also leverage expertise and university cooperation effectively.

DHS has developed a Countering Transnational Repression Engagement Plan to maximize the Department’s tools and authorities in countering TNR and its OPE has been engaged on this topic with various higher ed partners. Other DHS entities which are leading on addressing this issue and creating resources are HSI and OSLE. HSI’s Project Campus Sentinel provides school officials with an open communication channel to report any fraudulent activity or threats to national security, but it is unclear whether TNR has been properly defined or the reporting mechanisms defined well enough to make Project Campus Sentinel the appropriate channel for TNR reports.

There is also an FMI Working Group convened by the Office of the Director of National Intelligence (ODNI), which includes representatives from ODNI, NSC, DOS, DHS, FBI, DOJ, and the Department of Education, as well as several higher education associations. The working group is looking at how to best define FMI and TNR and engage institutions on these issues. Within DOS, the Bureau of Democracy, Human Rights and Labor is primarily focused on countering TNR and defending human rights and democracy abroad. They focus their efforts on four components: supporting coordination across USG agencies; providing education and training on TNR; engaging in accountability and deterrence efforts, such as imposing financial sanctions or visa restrictions; and building resilience in targeted

communities. There are also at least seven draft bills in Congress to address TNR and new tools to address the threat.

Creating too many communication channels, definitions, and best practices can lead to a fractured government response and a lack of clarity and understanding for colleges, universities, and students. In the worst case, a fractured response could even embolden malign actors engaged in TNR. On a positive note, because the federal government is at an early stage of recognizing and addressing this topic, we are at a pivotal point to bring various agency efforts into greater alignment and coordination.

**Addressing TNR is not a “one size fits all” approach. Aided by more transparent communication by government agencies to campus leadership, greater training and awareness, and clear points of contact, colleges and universities will be better equipped to detect and address incidents and support students and scholars who may be experiencing TNR.**

Overall, the briefers and reports noted the need for improved communications between campuses and government entities about TNR. University administrators lack sufficient awareness of the threats posed by certain foreign governments to members of their campus communities. Briefers communicated that reports are not routinely shared with academic institutions. Similar to research security incidents, unless law enforcement agencies proactively bring their campus points of contact into the fold when incidents involve their students, researchers, or faculty, campuses will never become properly informed or equipped to recognize TNR and combat it. Greater guidance and understanding of the threats posed by certain governments engaged in TNR activities would help colleges and universities make more nuanced determinations of risk, understand the prevalence on their campus, and implement risk mitigation measures.

The Subcommittee heard briefers express a desire for more training and awareness opportunities, as well as better coordination across various student-facing units so that TNR can be better understood and reported and so administrators can take appropriate steps to provide support, depending on the level of risk. It was noted that targeted individuals already feel isolated and alone in facing the pressure and consequences of TNR.

Lack of clear protocols for TNR unfairly places the onus for addressing TNR on the shoulders of those most vulnerable to it when there are many campus advocates who can be leveraged to provide timely support. It was acknowledged during many of our briefings that while university administrators are limited in their ability to truly “resolve” TNR, they can make a meaningful impact by making available additional resources to support students and faculty as they grapple with the complications of being a foreign scholar, including the risk of TNR. This could include sharing resources about asylum processes in the U.S.

Those with experience supporting affected students through incidents of TNR have emphasized that students who do report will first tell a trusted person in their network, which can be a faculty member, advisor, or staff liaison. This underscores the need for greater institution-wide awareness, so faculty and staff can recognize these phenomena and know how to provide support appropriately. Due to this dynamic, briefers noted that the

reporting of certain incidents may not require greater government involvement but rather equipping campus administrators with training and information on how to respond to the reports and support students. Briefers shared that if instances of TNR are reported to the institution, students may choose to remain anonymous for any reporting that goes beyond campus for various reasons, including their immigration status, uncertain future, risks to others including family if they report, and distrust of law enforcement.

While some briefers estimated that new campus reporting mechanisms would result in increased reporting, it should be noted that other briefers acknowledged that they did not have a sense of the scope of the TNR threats on campuses. They pointed to the variety of robust reporting mechanisms already available on campus, including anonymous reporting. These mechanisms are available to faculty, staff, and students, including mechanisms to refer students of concern and the full range of concerning incidents. These briefers noted that they receive nearly no reports related to TNR, whether through systems that identify students of concern, self-reporting by students, or anonymous reports. Another breifer noted the importance of building trust and relationships with students, so that they are more likely to report such incidents.

The absence of such reports may point to significant self-censorship being exercised by students coming from certain countries or their assumptions that having to deal with such threats is simply part of their experience as international students in the U.S. and so they do not share their experience with peers, mentors, faculty, or staff. On the other hand, it may be that the pervasive lack of awareness about TNR on campuses has obfuscated the “everyday threat” that certain international students face on U.S. campuses, as the 2024 Freedom House report asserts. Finally, briefers noted it is important to realize the limits of what can be resolved, and to not overpromise what the university can do, as that will lead to an erosion of trust between the student and the institution.

**The use of online tools and platforms, including social media, makes it easier to advance and spread TNR, and more difficult to track and identify perpetrators. Its targets can encompass individuals in diaspora communities and their family members remaining in the home country. This contributes to TNR being an underreported phenomenon.**

There are many methods foreign state actors use in employing TNR, ranging from spyware and family intimidation to renditions or assassination, but it is becoming increasingly impossible to measure the scale of TNR due to the rise of digital tools and technologies.

Student activists may not post or participate in discussion on platforms like WeChat — the most popular messaging and social media platform in China — because government malign actors are increasingly using online platforms like WeChat to harass, threaten, intimidate, and spread misinformation. WeChat accounts (known as Weixin inside China) are subject to widespread surveillance, much of which is enforced via China Communist Party mandates for China-based tech companies. Many Chinese international students studying in the U.S. use WeChat to form connections in the diaspora, engage in cultural activities, and connect with family in China.

Social media also allows for more spyware and for an environment of constant surveillance. For example, the Chinese Ministry of Public Security has a hotline where students can be reported for criticizing the government, which not only has psychological ramifications on visiting students but puts their families at risk back home.

There is not enough evidence to suggest that use of artificial intelligence (AI) deep fakes is a widespread risk in the TNR space, but AI could be leveraged to support surveillance or spyware tools that adversaries may use to intimidate, harass, and silence. Use of AI to accelerate TNR and its impacts is an area that the DHS and other agencies should be constantly assessing.

**TNR incidents threaten academic freedom and freedom of expression and as such, should be of concern to educational and research institutions.**

Academics and intellectuals who engage in research or advocacy deemed threatening to authoritarian regimes face intimidation tactics, including harassment, surveillance, and physical violence. This atmosphere of fear hampers academic inquiry and intellectual freedom.

Even in the case where there is no surveillance or where risk is low, the fear of retaliation can lead to self-censorship in opinions, research, and publications. In fact, by design, TNR is intended to have a chilling impact that extends beyond the individuals directly targeted. For example, it is used to intimidate and silence members of diaspora communities and family members who remain in their country of origin, organizations associated with human rights defenders, and civil society at large. This chilling effect stifles open discourse and inhibits the free exchange of ideas and as such, is of concern to institutions of higher education.

## RECOMMENDATIONS

DHS must strike a balance between protecting the international students who engage in our system of higher education from FMI while ensuring academic freedom and free and open discourse on campuses.

### RESEARCH SECURITY

**RECOMMENDATION #1: Inform universities of the threat landscape, trends, and update research security case studies.**

- Utilize the SECURE Center to disseminate research security guidelines and effective practices to institutions.
- Develop internal procedures to annually revise pertinent research security case studies to represent the current threat landscape. Be clear on risks and what we are trying to solve.
- Publish an annual assessment report of the threat landscape for universities which provides unclassified information and analysis of any new trends and data that emphasizes the problem (example: PP10043 enforcement trends). Account for risk mitigation in analysis of threats.

**RECOMMENDATION #2: Coordinate with other agencies on research security issues and utilize existing programs to engage universities.**

- Utilize the NCITF to coordinate and collect timely and consistent threat information that can be shared with universities.
- Strengthen coordination with the FBI academic liaison program to provide institutions a central point of contact for dealing with research security issues.
- Utilize Project Shield America and Project Campus Sentinel to hold briefings with institutions on current threats.
- Work with ODNI to publish resources as part of their Safeguarding Research Toolkit.
- Harmonize and implement common definitions developed by NSPM-33 and the NSTC Research Security Subcommittee.
- Harmonize reporting and compliance requirements across the federal government, similar to the implementation of common disclosure forms, to avoid a lack of consistency that creates a significant burden for universities to meet various different agency requirements.

**RECOMMENDATION #3: Engage with university, Asian-American, and other impacted groups to limit inadvertent harm from policies or enforcement actions on academic researchers. Consider staff training opportunities.**

- Seek engagement with higher education associations to help inform DHS policy decisions and avoid inadvertent harm to academic researchers, Asian-American scholars, or other impacted individuals.
- Develop and implement training for DHS Customer and Border Patrol officials to facilitate awareness building and understanding of the academic research environment to help maintain a welcoming environment for global students and scholars entering and re-entering the United States. This could include information on why students and scholars travel for research purposes and the value of international collaborations in research.

**TRANSNATIONAL REPRESSION**

**RECOMMENDATION #1: Develop a whole-of-government strategy to respond to issues of transnational repression.**

- Designate DHS and FBI as co-leads of a coordinated government approach. The FBI can serve as the lead for reporting and investigations. DHS can take point on developing and disseminating protocols, tools, resources, and best practices, including through Project Campus Sentinel, that campus leaders can reference.
- To support more strategic engagement with institutions of higher education and transparency around TNR, the federal government can:
  - Create a network of institutional points of contact dedicated to TNR, which would likely be those engaged in supporting international students and scholars (i.e., leads/senior international officers from Student Affairs or the Provost's Office).

- o Engage higher education associations and institutions about renaming TNR to stress transnational protections for students and scholars and protection of communities from interference.
- o Work with institutions to develop and disseminate a set of protocols, tools, and best practices, including best practices for receiving information from the community and a direct hotline for institutions to disclose reported incidents of TNR to their FBI liaisons and hold quarterly briefings for universities related to national security threats and updates on strategies to address cybersecurity threats.
- o Engage in diplomatic conversations with government and academic representatives from countries known for their TNR tactics.
- o Advocate for specific legislation aimed at protecting higher education from foreign influence and legal frameworks to establish international academic collaborations that do not compromise national security.
- o With public and private partners, support the development and refinement of policies that govern international collaborations to include protections for students and scholars from TNR.

**RECOMMENDATION #2: Compile resources and effective practices that help facilitate awareness building and identify training opportunities.**

- Working with various units within DHS, including OPE, and in collaboration with various higher education associations, develop and share resources and effective practices focused on increasing campus awareness of the prevalence of TNR and addressing it through various channels.
- Through outreach and engagement, OPE can encourage universities to help build awareness by educating their staff, faculty, and students about TNR, its tactics, and its impact, including how the fear of TNR may affect individuals from certain countries.
- Together with FBI and other DHS colleagues, OPE can also develop and share training modules for campus leaders, offices, students, and government agencies, including case study-based training for staff and faculty so that they can recognize and respond to potential instances of TNR. Training and awareness-building can take many forms:
  - o **Training module on TNR for international students.** Training can help define TNR, clarify the ways a student can report an incident on their campus, highlight university support services, and provide guidance on what a student may expect after reporting a TNR incident. Careful attention should be given on how to approach these training sessions, so they are inclusive, respectful, and do not play into stereotypes. While a training module may be introduced as part of new student orientation, the information provided in the training should remain easily accessible to students throughout their time on campus.
  - o **Training for faculty and instructors.** Training can help faculty understand the risks some students may be under, provide guidance on how to warn students

about the risks of TNR, build awareness of campus protocols related to TNR, and provide template language that could be used in syllabi.

- o **Training modules for relevant campus staff and offices.** This would primarily be directed to international student and scholar services, student affairs, counseling and psychological services, and academic support services. We further recommend that OSLLC should develop a video specifically for campus safety/security officers.
- o **Clear statements on the value of academic freedom and freedom of expression.** Universities and colleges can express solidarity with targeted students, staff, and faculty by making public their commitment to academic freedom and freedom of expression. The Subcommittee notes the example of Purdue University's statements and videos on academic freedom and freedom of speech. This includes the following message shared during international student orientation: "Everyone should understand that seeking to deny these freedoms to others, including by threatening them or suggesting that they might get in trouble back home if they exercise those rights here on campus, is unacceptable conduct at Purdue."
- o **Resource guides for international travel and other contexts.** The Subcommittee notes as an example the overview of TNR prepared by the University of Wisconsin at Madison for students and scholars engaged in international travel, which could serve as a sample template for others to follow.

**RECOMMENDATION #3: Designate agency and university points of contact and TNR reporting mechanisms to ensure two-way communication between the FBI, DHS, other agencies, and university administrations.**

- **Utilize the existing FBI academic liaison points of contact to share information and collect reports from colleges and universities.** The academic liaisons in FBI's regional offices are already a primary conduit for sharing information with institutions on research security. They can also leverage this outreach to track and follow up on TNR reports and ensure that proper lines of communication remain open to other agencies, including DHS and DOS. They can also ensure that information flows back to the university's point of contact so they can benefit from real-time information.
- **Higher education institutions should designate a point of contact for gathering reports of TNR from their campus community.** Higher education institutions may consider establishing an institutional committee to provide oversight of these mechanisms and of issues related to TNR and other forms of FMI with representatives from legal, security, research, and international affairs.
- **Higher education institutions should clarify campus reporting mechanisms for TNR.** At the time of this report, there is not yet one central and anonymous mechanism for reporting incidents of TNR nationally; however, each college and university should make clear how best to report threats to academic freedom or to their security. Institutions should consider explicitly naming and identifying TNR threats or harassment as incidents to report. The process for reporting TNR should be clear,



consistent, and easy to find, with options of anonymous reporting. There are examples of institutions that have adopted tools for this purpose, such as the University of Colorado using the Safe2Tell program, which allows anyone to make an anonymous report about threats and concerns. Those examples should be further studied to build effective practices.

**RECOMMENDATION #4: Institute timely data sharing so we can move beyond anecdotal reporting and develop better tools to quantify instances of TNR on campuses and inform subsequent actions taken.**

- So much of the information on TNR is based on anecdotes. The Subcommittee sees an opportunity for colleges and universities to work together with DHS and FBI to create a clearing house, potentially based at a major university or a related higher education association, to facilitate the sharing of information, to create a database that can be available to universities in real time, and to help determine best practices related to reporting incidents.

## **OVERARCHING RECOMMENDATIONS**

**RECOMMENDATION #1: Look to the past to inform the future. The evolution of coordination between higher education and government agencies can provide lessons to inform a framework for a measured, transparent, and consistent approach for both research security and TNR.**

As was noted earlier in this report, early collaboration between federal agencies and higher education institutions on research security issues were hampered by a lack of clarity on a central point of contact for managing such issues and lack of early engagement and coordination with the higher education sector as a thought partner to develop evidence-based effective practices and clear, consistent guidance. It took years to develop better coordination between USG agencies and higher education institutions, as well as a more systemic approach. These concerns led to the creation of the academic liaison program at the FBI, which strengthened coordination between the FBI and universities and promoted the sharing of information on emerging threats and concerns. Several briefers note this has been an effective coordinating mechanism and could also be a model for engagement when it comes to TNR and other issues.

In addition to a central point of contact, there are other common themes from the research security collaboration that would be beneficial to apply to the approach to TNR. While these may be mentioned elsewhere in the report, we offer a summary of them here. Both TNR and research security would benefit from:

- Harmonized and consistent definitions;
- Clear statements of threats and development of risk levels;
- Transparent decision processes and points of contact;
- Awareness raising, training, and education;
- More proactive outreach from government agencies and real-time information sharing; and

- Harmonization of forms, definitions, and reporting across the USG.

**RECOMMENDATION #2: The nation must continue to invest in strengthening our research and education institutions, which are the bedrock of our national security, and support the recruitment and retention of top talent to ensure U.S. competitiveness.**

America's research and innovation ecosystem is powered by higher education, which serves as an extraordinary engine of social mobility and catalyzes our nation's economic prosperity. This enterprise has been successful because of the dedication and contributions of all of our scholars and students, many of whom come from all over the world. We must ensure that our research ecosystem remains strong, which requires a steadfast commitment to the free flow of ideas and the development of the world's top talent.

A fundamental component of building the resilience of U.S. higher education must be an increased investment in domestic science, technology, engineering, and math (STEM) talent. This means increased federal investment in the research capacity, teaching, and resources of the colleges and universities educating most of the students who are currently underrepresented in STEM fields, including Hispanic Serving Institutions (HSIs), Historically Black Colleges and Universities (HBCUs), Tribal Colleges and Universities (TCUs), and community colleges. Domestic students, including first- and second-generation immigrant students, are essential to filling critical workforce needs and realizing the benefits of our national technology and innovation priorities, such as the CHIPS and Science Act. We recommend that DHS seek engagement with higher education associations to help inform DHS outreach and policy priorities in this regard.

At the same time, the U.S. has always been at the cutting edge of countless fields precisely because we have kept our doors open to the best and brightest from around the country and around the world. As a nation, we must prioritize immigration policies that are central to continuing our global work, deepening our commitment to national security, and supporting the recruitment, student success, and retention of international students, scholars, and alumni who are integral and valued contributors.

## CONCLUSION

There have been many promising developments made in recent years to strengthen the collaboration between higher education and the federal government to counteract FMI in higher education. The Subcommittee applauds the work that has been advanced.

We hope this report underscores the importance of maintaining vigilance and pursuing collaboration when it comes to research security and TNR, and sheds light on the urgent need for robust cooperation to mitigate the risks posed by FMI in higher education. As we navigate an increasingly interconnected world, it is imperative that DHS and constituencies across academia, civil society, and policymaking spheres remain proactive in defending the principles of academic autonomy and human rights, thereby fostering a conducive environment for scholarly inquiry and innovation to thrive.

## APPENDIX 1: TASKING LETTER

*Secretary*

**U.S. Department of Homeland Security**  
Washington, DC 20528



**Homeland  
Security**

November 14, 2023

MEMORANDUM FOR: Elisa Villanueva Beard  
Chair, Homeland Security Academic Partnership Council

CC: Dr. Walter Bumphus  
Vice Chair, Homeland Security Academic Partnership Council

FROM: Alejandro N. Mayorkas  
Secretary

SUBJECT: **Formation of a New Homeland Security Academic Partnership Council Subcommittee and Tasking it to Provide Recommendations Regarding Foreign Malign Influence in Higher Education**

I greatly appreciated our inaugural meeting on September 6, 2023. As I noted during our discussion, I request that the Homeland Security Academic Partnership Council (HSAPC) form a subcommittee to evaluate and provide recommendations around foreign malign influence in higher education institutions.

I request that the HSAPC submit its findings and key recommendations to me no later than 150 days from the date of this memorandum, consistent with applicable rules and regulations.

### **Foreign Malign Influence in Higher Education**

Academic partners provide valuable insights into the Department of Homeland Security's most pressing issues, including domestic violent extremism, transnational criminal organizations, cybersecurity, and the homeland security implications of climate change. As the threat environment the nation faces continues to evolve, the Department must consider how to better leverage the insights and research capabilities of U.S. academic partners to help address emerging and evolving threats.

Foreign malign influence is a threat to our national security and is particularly concerning at our nation's colleges and universities when it involves intellectual property theft and transnational repression. Foreign adversaries are increasingly seeking to exploit our higher education institutions as platforms for their own gain at home and abroad.

Malign actors at times may perceive colleges and universities and their inherent promotion of academic freedom and openness as a threat to their own national interests and policies. The colleges and

universities may also be seen as a forum to promote the malign actors' ideologies or to suppress opposing worldviews. In addition, accessing higher education institutions presents an opportunity to steal research and technology for the malign actors' own aims.

Malign actors employ various tactics to achieve foreign malign influence, including monitoring, intimidating, and threatening students on U.S. campuses-or targeting the overseas families of international students attending U.S. institutions-to silence dissenting views; persuading or pressuring academics to self-censor views they might oppose; influencing publications they view as denigrating to their own interests or views; funding research and academic programs, both overt and undisclosed, that promote their own favorable views or outcomes; and stealing the resources, expertise, and products of academic research conducted at colleges and universities. This infiltration undermines the trust and transparency essential to maintaining the integrity of our education system. This jeopardizes U.S. national security and the free exchange of ideas.

DHS reporting has illuminated the evolving risk of foreign malign influence in higher education institutions. One such example is the Chinese Government's efforts to regain influence in U.S. universities by concealing its connection to Confucius Institutes. These institutions were rebranded as non-governmental organizations (NGOs) in 2020 following accusations that they suppressed academic freedom and promoted Chinese Government propaganda. The NGO status was used to undermine transparency in international collaborations, including clear disclosure of funding sources and rigorous vetting of foreign partners, and complicated the ability of higher education institutions and the U.S. Government to identify, track, and address potential risks.

Foreign malign influence at universities is not unique to the United States, and our allies and partners have developed their own guidance to address this challenge. For example, in 2019, the Australian Government developed Guidelines to Counter Foreign Interference in the Australian University Sector that promote frameworks and policies to identify and mitigate threats of foreign interference and to promote, support, and strengthen the resilience of higher education institutions.

Given the need to accelerate and further enhance U.S. academic resilience in the face of this evolving threat, I request that the HSAPC form a subcommittee to review and provide recommendations for mitigating foreign malign influence at our colleges and universities, taking into account existing prevention frameworks and models from the public and private sectors. Specifically, the review and recommendations should include:

- Guidelines and best practices for higher education institutions to reduce the risk of and counter foreign malign influence;
- Consideration of a public-private partnership to enhance collaboration and information sharing on foreign malign influence; and
- An assessment of how the U.S. Government can enhance its internal operations and posture to effectively coordinate and address foreign malign influence-related national security risks posed to higher education institutions.

## APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES

Name	Title	Organization
Emraan Ansari	Policy and Advocacy Officer	Freedom House
Dr. Fanta Aw	Vice President of Campus Life, Executive Director, and CEO	American University and NAFSA – Association of International Educators
David Biggs	Lead Officer for Research Integrity and Security Issues, Office of Science and Technology Cooperation, Bureau of Oceans and International Environmental and Scientific Affairs	DOS
Annie Boyajian	Vice President for Policy and Advocacy	Freedom House
Josh Dermott	University Counsel	Georgetown University
Jack Glore	Intelligence Research Specialist	DHS Office of Intelligence and Analysis
Alisa Hall	Acting Screening Division Chief in the Office of Screening, Analysis, and Coordination, Bureau of Consular Affairs, Office of Visa Services	DOS
Mariah Hicks	Law Enforcement Program Manager	OSLLE
Mark Howard	Director for the Office of Private Sector Exchange Program Administration, Bureau of Educational and Cultural Affairs	DOS
John Iorio	Executive Director	OSLLE
Gisela Perez Kusakawa	Executive Director	Asian American Scholars Forum
Sarah Stalker-Lehoux	Deputy Chief of Research Security Strategy and Policy	U.S. National Science Foundation
Dr. Xihong Lin	Professor, Coordinating Director of the Program in Quantitative Genomics, Harvard University	Asian American Scholars Forum

Peter Marigliano	Consular Intelligence Coordinator, Bureau of Intelligence and Research	DOS
Susan Martinis	Vice Chancellor for Research and Innovation	University of Illinois
Kevin Mayner	Foreign Service Officer, Bureau of European and Eurasian Affairs	DOS
David Norton	Vice President for Research	University of Florida
Paul David Plack	Senior Policy Advisor to the Deputy Assistant Secretary for Academic Programs, Bureau of Educational and Cultural Affairs	DOS
Lauren Protentis	Director of Countering Foreign Malign Influence	White House, National Security Council
Lauren Raskin	Foreign Affairs Officer, Bureau of Democracy, Human Rights, & Labor	DOS
Roman Rozhavsky	Section Chief of the Counterintelligence Division	Federal Bureau of Investigations
Rob Rutenbar	Senior Vice Chancellor for Research	University of Pittsburgh
Nate Schenkan	Senior Director of Research, Countering Authoritarianism	Freedom House
Peter Schiffer	Dean of Research	Princeton University
Susan Schneider	Branch Chief for Active Assailant Security	Countering Transnational Repression, Office of Partnership and Engagement
Steven Schultz	General Counsel	Purdue University
Katherine Sermersheim	Vice Provost for Student Life	Purdue University
Halley Smith	Unit Chief for Technology in the Office of China Coordination, Bureau of East Asia & Pacific Affairs	DOS
Erik Smulson	Vice President for Public Affairs and Senior Advisor to the President of Georgetown University	Georgetown University
Grady Vaughan	Research Associate	Freedom House
Andre Watson	Director for National Security	Homeland Security Investigations

Jeannette Wing	Executive Vice President for Research	Columbia University
----------------	---------------------------------------	---------------------