¶1320.15 *International Collaboration with Foreign Influence Risk*

Roseann Luongo, Huron Consulting Group, James Luther, Duke University and Scott McGaunn, FBI

International research is more important than ever today – yet it's also undergoing immense scrutiny. With the increasing number of foreign influence threats at colleges and universities, American intellectual property is at an elevated risk of interference, in addition to the general state of collaboration between countries. While institutions in the United States must keep working with foreign countries on research and development in the name of global improvement, there are certain steps and precautions they can take to ensure data and sensitive information is protected.

In August 2018, the National Institutes of Health (NIH) started to issue letters to institutions, reminding applications that they, "…must disclose all forms of other support and financial interests, including support coming from foreign governments or other foreign entities" and altering them that they may receive inquiry form the Office of Extramural Research (OER) related to specific "…applications, progress reports, policies, or personnel" related to their institution. NIH has performed foreign influence investigations and has reached out to institutions directly with specific inquiries and many of them have resulted in criminal complaints filed by the Department of Justice resulting in arrests, institutional return of funds and fines.

At the same time, the Office of Inspector General (OIG) at the National Science Foundation (NSF) investigated and recommended sanctions on 16 to 20 cases and referred an undisclosed number of criminal and civil cases to the Department of Justice.[1] While most of the researchers were U.S. citizens, all but two of these cases involved ties to China. Some grant recipients spent several months a year outside of the U.S., while others engaged in "double dipping" – the act of receiving outside support for research that was already covered by an NSF grant.

The investigation outcomes included the researchers being terminated by their institutions and barred from applying for future funding, the institutions returning the funds, and the NSF reassigning, suspending, or terminating the grants.

These incidents have repercussions greater than just the monetary loss. Some foreign governments seek intellectual capital, ideas, and information on grant proposals. Some techniques may not be illegal; however, they are unethical and lack transparency and reciprocity. This includes the unauthorized sharing of pre-publication research data by faculty and students, acquiring advanced access to grant proposals, and influencing the grant approval process.

In addition to agency action, the Senate has recently passed a bill with bipartisan support. The goal of this bill is to protect U.S. research and development and intellectual property. This bill proposes implementing sanctions for the theft of U.S.-funded IP, establishing federal grant application as a federal crime, and banning federal investigators from participating in Talent Programs.[2] Legislative and Executive

[1] *Nature*, US National Science Foundation Reveals First Details on Foreign Influence Investigations (July 7, 2020)
[2] S.1260 - United States Innovation and Competition Act of 2021

branch actions to combat foreign influence have spanned both the Trump and Biden administrations and institutions should anticipate this action to continue. Congressional support to reduce foreign influence risk has bi-partisan support, institutional and research administrators should continue to pay attention to federal agency and legislative activity surrounding foreign influence as it continues to evolve.

The FBI's Counterintelligence Efforts

The Federal Bureau of Investigation (FBI) recognizes that a collaborative, open, and inclusive academic environment promotes life-changing research and fosters cooperation between nations. With U.S. universities and their foreign partners driving innovation and economic growth, and international students and scholars contributing significantly to U.S. research and the economy, it is imperative to advance international collaboration. However, it is also important to do so safely and carefully to protect U.S. intellectual property (IP).

The cutting-edge research and technologies that are being developed here in the United States must be carefully protected from our foreign adversaries and the FBI will continue to do everything it can to safeguard these important innovations.

The ruling Communist Party of the People's Republic of China is engaged in an unprecedented long-term campaign of espionage and intelligence collection against American businesses, universities, research facilities, and other sensitive locations. There is nothing speculative about this concern. As FBI Director Christopher Wray recently told Congress, "There is no country that poses a more severe counterintelligence threat to this country right now than China."

China is considered the United States' primary adversary in the counterintelligence field. Director Wray emphasizes that the FBI targets behavior, not ethnicity, when it comes to counterintelligence efforts. He also stated, "…China is fighting a generational fight here. And when I say China, I want to be clear, this is not about the Chinese people as a whole, or the Chinese Americans in this country. What it is about, though, is a variety of ways the Chinese Communist Party is using government officials, private sector entities…to steal their way up the economic ladder at our expense. The threat is deep and diverse and wide and vexing. It affects basically every industry in this country."

Considering the information that some institutions have access to – like research into military technology – colleges and universities must protect sensitive information, even if it's unclassified. Foreign intelligence officers being privy to this type of research can have serious national security and economic implications. There are known cases of Chinese intelligence services having recruited academics and students while traveling in China. The academic colleagues and government contacts a person can meet while travelling to China may be intelligence officers operating under the guise of academic exchange. Contact with a targeted academic is often first made through professional networking websites, foreign conferences, and networking events.

Chinese theft of research and technology costs our country between $225 billion and $600 billion a year. China-related intellectual property theft and economic

espionage matters are being investigated in all of the FBI's 56 major field offices. To put this threat into perspective, we have now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours. And of the 5,000 active counterintelligence cases the FBI has, nearly half of them are related to China. And what needs to be made clear is that the Chinese Communist Government doesn't play by the same rules of academic integrity and freedom that we do.

We know they use some Chinese students in the U.S. as "non-traditional collectors" (untrained, non-governmental intelligence assets) to steal our intellectual property. We know that through their "Thousand Talents Plan" and similar programs, they try to entice researchers at our universities to bring their knowledge to China—even if that means stealing proprietary information or violating export controls or conflict-of-interest policies to do so.

We also know they support the establishment of institutes on our campuses that are more concerned with promoting Communist Party ideology than independent scholarship. They try to pressure Chinese students to self-censor their views while studying here, and they use campus proxies to monitor both U.S. and foreign students and staff. And we know they use financial donations as leverage, to discourage American universities from hosting speakers with views the Chinese Communist Government doesn't like.

The FBI seeks out those that are involved in such malign foreign influence, and those that may be sharing or providing intellectual capital that the U.S. government has already funded. Within the Greater Boston region we have seen China take a broad approach to these efforts, using not just intelligence officers but academics, businesspeople, students, and other civilians to achieve its strategic objectives. We know that students at Boston-area universities have stolen biological intellectual property and materials from university laboratories in order to bring the materials back to China. We also know that in the past the Chinese People's Liberation Army (PLA) has planted intelligence agents, posing as university students, at Boston-area universities and tasked them with obtaining information about research processes and faculty.

China is trying to fill its strategic gaps at the expense of other nations. As outlined in its own Made in China 2025 initiative and most recent Five-Year Plan, China is striving for self-sufficiency in key research and technical sectors, and it is doing so by stealing technology from foreign countries, replicating it for domestic use, and then replacing the original, foreign tech with its own, first in the domestic market and then globally.

We rightly celebrate the culture of openness in US academia, and foreign visitors who study, innovate, and start businesses here make our country stronger. We know that most Chinese students and researchers in the United States are here for legitimate academic purposes. But some are not. The Chinese government routinely recruits some percentage of Chinese nationals and others to assist in intellectual property theft.

The breadth and scope of the coordinated efforts of private and governmental forces in China to drain our country of intellectual capital is truly staggering. We must likewise embrace a holistic approach to countering the threat. Federal authori-

ties routinely develop partnerships with private institutions to enhance awareness, and we all share the goal of confronting this problem while maintaining a welcoming atmosphere for foreign researchers. Universities and businesses should urge transparency in dealings with foreign entities, including the Chinese government. Federal agents and prosecutors cannot do the job alone. The Government needs the support and partnership of the entire academic ecosystem to mitigate the threat of wholesale foreign IP theft from our country.

Current Landscape and the Unpreparedness of U.S. Institutions

While many institutions have led efforts to manage foreign influence and respond to federal disclosure requirements, some institutions are still struggling to develop formal risk management efforts related to foreign activities.

Institutions who receive Department of Education Funding were reminded that the agency has a reporting requirement under Section 117 of the Higher Education Act of 1965. Section 117 requires that institutions report on any gift from or contract with a foreign source that has an aggregate value of $250,000 or more within a calendar year. Institutions with Department of Education funding need to make sure that they understand compliance requirements regarding gift acceptance, agreement and contract execution, and management. They also need to engage institutional stakeholders to strengthen processes and controls related to foreign gift and contract reporting and coordinate across the institution to ensure timely and accurate reporting of funding.

While Section 117 specifically covers foreign gift giving (any monetary value over $250,000), the new NIH guidance that was released expands this to include any resource or financial support, from all foreign or domestic entities. It covers all research resources available – including grants or donations made in-kind, like equipment or even housing.

The NIH and NSF have recently released guidance that helps to clarify reporting and disclosure requirements related to foreign influence. The NIH notice, published on March 12, 2021 provided updated requirements for biosketches and Other Support with an effective date of May 25, 2021. The NIH subsequently published a notice on April 28, 2021, that moved the implementation date from May 25, 2021, to January 25, 2022. The key takeaways from the NIH notice are as follows:

- Supporting documentation for foreign activities and resources included in Other Support must be provided (e.g., contracts, award notices, etc.), including a translated English copy if the original document is in another language.
- Institutions must determine whether they want to collect contracts through the COI and COC disclosure process, and if so, how those contracts will be provided to pre-award teams.
- Institutions must immediately notify the NIH Grants Management Specialist if the institution learns of Other Support that was not disclosed.
- Institutions should determine their risk tolerance for reviewing COI / COC disclosures during proposal submission process; if reviewing, they should also see what COI systems access can be provided to pre-award teams.

- Accuracy of the Other Support information submitted must be certified by the Program Director/Principal Investigator or Other Senior/Key Personnel prior to submission.

The NSF also recently released an updated policy guide for NSF Pre-award and Post-award Disclosures related to Biographical Sketch and Current and Pending Support. It is critical that institutions evaluate their Other Support, biosketch, and Current and Pending disclosure processes to ensure that they are able to timely and accurately:

- Identify Other Support data sources.
- Consider using a technical solution to pull disparate data sources.
- Determine how to validate faculty disclosures.
- Establish internal review process to ensure data accuracy and consistency.

Federal funding agencies have made it clear that they want to know about investigator activity outside of their institutional primary appointment and how their research portfolio is funded, both through direct outlays and in-kind contributions. Institutions need to evaluate their current processes and data to ensure that they are collecting the appropriate information from investigators so that they can comply with federal disclosure requirements. Federal agency requirements for foreign influence disclosure requirements continue to evolve and research administrators should continue to monitor agency guidance and industry updates on these topics.

Protecting University Research

Given the increase in such cases, the FBI has been conducting more outreach to universities to develop deeper partnerships. That way, if an institution identifies an issue they can work directly with the FBI on potential conflicts of interest and decide how to best move forward. Furthermore, moving forward does not always entail an FBI response. These matters can often be clarified and mitigated through the relationship developed with the university's executives and general counsels, along with their local FBI partners and grant funding agencies. Likewise, if it is the FBI that discovers potential wrongdoing, they can often engage with the university to determine a reasonable course of action, depending on the nature of the wrongdoing and the actors involved. Local FBI offices are prepared to offer mitigation strategies, recommend reliable resources for foreign influence risk identification, and provide briefings to administrators, faculty and students on current and emerging risks.

With institutions being the ones to report this information, it is crucial to properly educate faculty and researchers on the types of information they need to disclose. Universities should encourage open communication between leaders, principal investigators, and researchers on what is required to report, and how it impacts the institution. Failure to completing and accurately disclose can result in fines, penalties and enforcement activity for the individual, and in cases where it has been determined that the institution was aware of incomplete or inaccurate disclosures then the institution may also face fines, penalties and enforcement activity.

Institutions should rethink what their administrative structure is to manage these compliance requirements. Typically, with conflict-of-interest cases, one functional area reports on the disclosures, and the other is the one that sees this firsthand. These areas are siloed and are not actively collaborating and collect information separately. In the future, they need to be more coordinated to have a more comprehensive picture of the risk. This will require expanded data transparency of information that has historically been small group of people with COI and compliances offices that are separate from the operational pre-award and departmental grant management teams that manage proposal, Just-In-Time and Other Support submission. The lines between the operational and compliance teams have become blurred as reporting and disclosure requirements across both areas have started to merge.

As an institution evolves, its structure needs to evolve as well. In the moment, it can be difficult to determine what is needed to report on and submit – and institutions are struggling with doing it efficiently, effectively, and timely. Today, there are specific roles for tasks that previously were left to the last minute. Colleges and universities that lack this kind of capability in-house can work with will struggle to coordinate between disparate roles and systems to leverage existing data, gather expanded data requirements to maintain compliance and meet deadlines.

In an effort to manage foreign influence risk, some institutions have expanded background checks for visitors and employees who may work on research projects to ensure they understand who is working on projects and what they will have access to. Visitor access has long been an area that institutions needed to manage to ensure that Visiting Scientist agreement templates to capture technology and space access, IP restrictions, disclosure requirements and that the appropriate approvals and controls were in place to manage access, foreign influence has presented a renewed focus on visitor access.

Additionally, institutions should consider travel monitoring to review where faculty and researchers frequently travel and compare this to disclosure data to determine if there are gaps in disclosures that require additional follow-up.

There are additional considerations for higher education leaders. Existing risk management and compliance programs should be strengthened—and in some cases, added to— to support this work. Leaders should assess risk to an institution's sensitive technologies, research and develop a plan to protect them accordingly, and decide if more resources are needed. These teams should secure data and information and ensure agreements for joint research programs protect data. They can also vet research partners and evaluate existing foreign access to laboratory and computing resources.

The following table outlines key actions that institutions can assess across the lifecycle of sponsored funding in order to reduce foreign influence risk.

Lifecycle Area	Actions to Consider
Proposal Submission	• Include foreign components in proposal • Ensure biosketch/SciENcv is complete and accurate
JIT	• Explore system solutions for gathering and reporting data at the Just-In-Time phase to increase consistency and reduce duplication of effort

Lifecycle Area	Actions to Consider
COI + COC	• Review COI and COC disclosures to determine if information internally disclosed requires agency disclosure
Award Management	• Monitor travel via GL, SOS programs and institutional booking programs to identify abnormal patterns • Request prior approval for new foreign components • Consider use of loaner laptops and phones when traveling abroad, certain website blocking and limitation on USB ports.
Reporting	• Establish processes to ensure compliance with agency reporting requirements • Perform risk-based monitoring on reported data to ensure data integrity • Collaborate with departments across the institution
Award Closeout	• Ensure all reporting is complete and accurate • Document award compliance

Balancing International Collaboration with Foreign Influence Risk

This is all underscored by the need to continue to collaborate internationally. Many universities have come forward to say as much – releasing open letters and advocating to the government. There is no question that this must continue: if the United States starts becoming very isolated and does not collaborate with other countries, U.S. research would suffer long-term. It is important that the country is able to maintain and continue collaboration with all other nations and partners across the globe.

To continue to collaborate internationally, there needs to be enhanced transparency. Disclosing research partners and why they are involved can help the NIH and other sponsors make funding decisions and ensure the U.S. funds research that the investigator has the capacity to perform. It also provides sponsors with an opportunity to evaluate recipient controls to ensure that U.S. funded intellectual property is protected.

While foreign influence risk has increased more, the global imperative to continue to work together has never been stronger. We see this in key moments throughout history, like the COVID-19-pandemic or the world's ongoing battle with climate change. The ability to share perspectives and ideas, cultural interactions and knowledge can still be celebrated and encouraged while doing so safely. And as colleges and universities are bastions of research and scholars, they are the first to really pursue this trial-and-error approach. Striking the right balance between collaboration and precaution will take time but ultimately will lead to further growth and better cooperation in the future.

About the Authors

Roseann Luongo is a consultant with Huron Consulting Group and an adjunct faculty member with the Emmanuel College Research Administration graduate program. She has over 19 years of experience in research compliance and administration, including risk assessment, policy and process development, compliance concern investigation, and conflicts of interest analysis and management. She can be reached at rluongo@hcg.com

Jim Luther, the Duke University Associate VP Finance & Research Costing Compliance Officer is responsible for compliance management & monitoring and is the

institutional sponsor liaison. He is the past-Chair of the Board of the Council on Governmental Relations (COGR) and is the co-chair of the Finance/Compliance Committee for the Federal Demonstration Partnership (FDP). He can be reached at james.luther@duke.edu

Scott McGaunn has been an FBI Special Agent for the past 26 years. He has extensive experience in intellectual property, terrorism, organized crime, cyber-crime, and counterintelligence investigations. Special Agent McGaunn is currently engaged in creating strategic partnerships between the FBI, academic institutions, and corporations throughout New England. He can be reached at spmcgaunn@fbi.gov