COGR

Council On Governmental Relations

An Association of Research Institutions

Federal Focus on Inappropriate Foreign Influence on Research:

Practical Considerations in Developing an Institutional Response

August 18, 2021

This Framework is provided as a tool to the COGR Membership with the understanding that COGR is not providing legal, regulatory, or policy advice.

Acknowledgements

Many thanks to the team of COGR members and COGR staff who contributed to the completion of this paper.

Project Team

Elizabeth Peloso, Associate Vice President & Associate Vice Provost, Research Services, University of Pennsylvania (*Lead)*

Robert Hardy, Director Research Security and Intellectual Property, COGR (*Co-lead)*

Allen DiPalma, Director, Office of Trade Compliance, University of Pittsburgh

Naomi Schrag, Vice President for Research Compliance, Training, and Policy, Columbia University

Kris West, Director Research Ethics and Compliance, COGR *(Co-lead)*

COGR
Council On Governmental Relations
An Association of Research Institutions

Table of Contents

Introduction

Over the past several years there has been increasing concern about potential malign foreign influence and research security risk at U.S. research institutions. These concerns encompass a variety of activities such as: nondisclosure of foreign gifts to and contracts with U.S. academic institutions; recruitment of U.S. scientists to participate in foreign government-sponsored talent programs (FGTPs) that support the development of critical emerging technologies; and theft of intellectual property and/or diversion of intellectual capital developed with U.S. government funds at U.S. research institutions. While certain countries, including Russia, Iran, and others, have caused concern, the U.S. government's primary focus has been on the People's Republic of China (China), as illustrated by FBI Director Christopher Wray's February 2018 address before the U.S. Senate Intelligence Committee in which he stated that the academic sector was naïve to the China threat.[1]

Since 2018, Congress and U.S. funding agencies have taken, and continue to take, action to address the perceived threat that the open U.S. academic environment poses to research security. Some of these actions apply specifically to research institutions and others apply more broadly to all recipients of federal funding. The following non-exhaustive list sets forth some of the governmental actions that have had significant impact on the COGR membership:

- Prohibition on purchase or use of telecommunications equipment produced by certain Chinese manufacturers per Section 889 of the 2019 John S. McCain National Defense Authorization Act and implementing regulations
- Addition of new restricted entities to federal restricted party lists, including additional non-U.S. universities
- Expanded requirements for, and enforcement of compliance with, the Department of Education requirements for reporting of gifts and contracts from foreign entities by recipients of Title IV funding under Section 117 of the Higher Education Act of 1965 (20 USC §1011f)
- New guidance on the reporting of foreign affiliations and activities in Biosketch and Other Support reports to the NIH with, in some cases, suspension of grant participation pending investigations of potential FGTP participation (*see, e.g.,* NIH NOT-OD-21-073)
- New guidance on the reporting of foreign affiliations and activities for National Science Foundation grants (*see, e.g.,* "NSF-Approved Formats for Current and Pending Support" webpage))
- Increased requests for detailed information and/or prior approval of the participation of foreign nationals in research contracts (*see, e.g.,* Department of Energy Order 486.1A and Undersecretary of Defense March 20, 2019 Memorandum)
- Office of Science and Technology Policy (OSTP) review resulting in the issuance of National Security Policy Directive 33 in January 2021 (NSPM-33)

In addition to NSPM-33, the OSTP National Science and Technology Council Joint Committee on the Research Environment (JCORE) Subcommittee on Research Security issued an

[1] Transcript of Open Hearing on Worldwide Threats (S. Hrg. 115-078), Select Committee on Intelligence, U.S. Senate, February 13, 2018.

accompanying guidance document to assist research institutions with establishing research security programs: "Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise" ("JCORE Guidance"). While the JCORE Guidance advocates for a risk-based approach to research security and incorporates many good practices previously identified as common at research institutions, it also lists practices not currently in use at many institutions. Further, although the JCORE Guidance is framed as presenting "recommendations" to institutions, it remains to be seen whether agencies instead may view them as baseline requirements. In all events, the cost and administrative burdens associated with implementation of the JCORE Guidance may be substantial, although they will differ among institutions depending on their research portfolio and risk assessment.

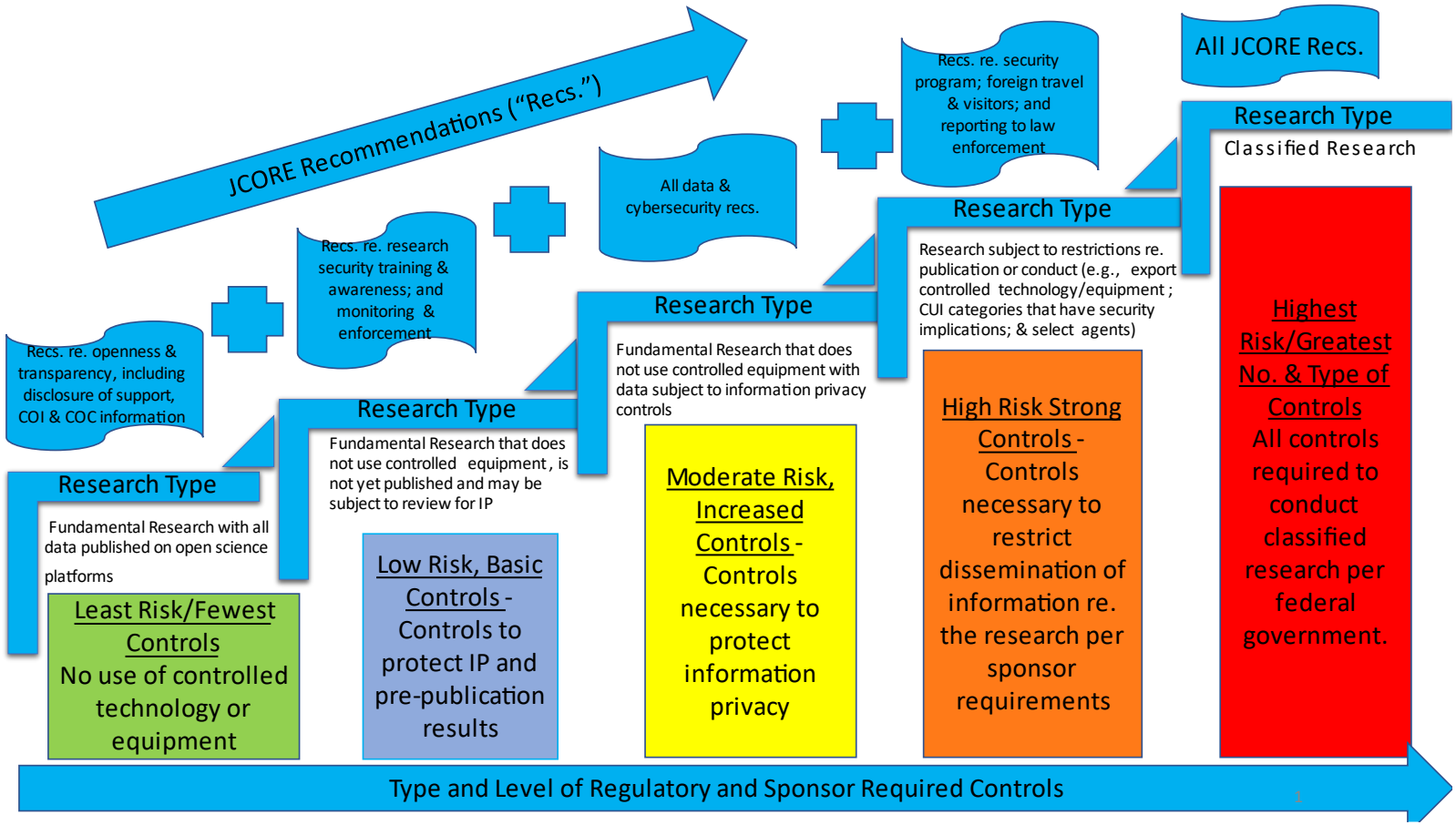
On August 10, 2021, OSTP announced the start of a 90-day initiative to "develop clear and effective implementation guidance for NSPM-33" that will address agency requirements for disclosure policies, oversight and enforcement, and research security programs.[2] Spurred on by GAO reports[3] urging agency action on malign foreign influence, federal research funding agencies had already started to implement NSPM-33, and in doing so acknowledged the benefits of inter-agency harmonization of requirements for institutional research security. As these requirements begin to stabilize, research institutions are performing risk analyses, assessing current security programs, and determining where changes will need to be made. This white paper seeks to provide information and points institutions should consider on issues related to research security as they undertake these reviews, with the recognition that security programs will differ depending on an institution's mission, the size and character of its research portfolio, and available institutional resources. Although institutional responses will vary, institutions should review the points identified in this paper when performing risk assessments and develop processes to appropriately address areas of higher research security risk.

A Risk-Based Approach to Research Security and the Management of International Collaborations

Science does not have borders, and international collaborations among scientists are essential to the success of both academic research institutions and scientific advancement as a whole. Further, unlike commercial enterprises, one of the primary goals of academic institutions is to generate and disseminate knowledge freely. Nevertheless, as recent government investigative efforts have revealed, not all countries play by the same rules of information-sharing and transparency, creating risks to the U.S. research enterprise and its funding agencies. Accordingly, institutions and government agencies must take a "balanced, risk-based approach [that] recognize[s] the benefits of open, international collaboration, as well as the risks" to scientific integrity and research security.[4] Efforts to strike this balance are particularly important in fundamental research, which, by definition, is intended to be published and shared. A possible broad-based model for implementing the JCORE Guidance in a risk-based fashion to different categories of research appears in the figure on the next page. This model demonstrates that as research risk increases, controls should simultaneously increase.

[2] Lander, E., "Clear Rules for Research Security and Researcher Responsibility" (Aug. 10, 2021).
[3] GAO-21-523T (Apr. 22, 2021); GAO 21-130 (Dec. 17, 2020)
[4] JCORE Guidance, p. 4.

Figure 1: Potential Model for Risk-Based Application of JCORE Recommendations & Controls



COGR's "Framework for Review of Individual Global Engagements in Academic Research Managing Conflicts of Interest and Conflicts of Commitments in the Context of Undue Foreign Influence Concerns" takes this risk-based approach to a more detailed level by providing a structured approach for analyzing individual international activities that institutions or their researchers are considering. The Framework lists risk factors and poses a series of questions that institutions can use in their evaluation, along with potential risk mitigation strategies. Risk assessment must consider the nature of the activity and the various types of risk involved (e.g., reputational, financial, legal) to determine if the risk can be mitigated or must be avoided altogether. Further, in the case of mitigation, the Framework considers possible mitigation vehicles, e.g., contractual approaches such as termination clauses or representations and warranties, full transparency regarding the research relationship and results, clear delineation of institutional and individual researcher activities, etc.

Managing Conflicts of Interest and Conflicts of Commitment to Address Inappropriate Foreign Influence

One area of particular focus for funding agencies is the promulgation of additional guidance regarding researchers' disclosure of external activities or sources of support that may present financial conflicts of interest or conflicts of commitment (sometimes referred to as "non-financial conflicts of interest") and may also pose a risk of inappropriate foreign influence. Funding agencies have expressed concern regarding researchers' participation in certain FGTPs that have problematic contractual requirements such as committing to substantial employment with foreign entities or provision of unpublished research results or intellectual capital to a foreign government. In some cases, researchers have intentionally failed to disclose participation in these FGTPs, making it impossible for institutions and funding agencies to determine if there is inappropriate overlap of science, commitment, or funding. Even in areas of fundamental research where results will ultimately be published, funding agencies have made clear that scientific integrity is negatively impacted when there is a lack of transparency, or in some cases deceit, about research support and researcher commitments.

Agencies have expressed their concerns regarding FGTP programs and made clear that researchers must be transparent about all research-related positions, appointments, and support and that institutions should be aware of their researchers' activities. For example, NIH issued several notices and FAQs pertaining to changes in the format of Biosketch and Other Support reporting,[5] including the following new requirements: (a) certification by both the investigator and the institution as to the accuracy of Other Support disclosures; and (b) submission to NIH of copies of agreements specific to senior/key personnel's foreign appointments and/or employment with a foreign institution for all foreign activities and resources reported as Other Support.[6] NSF also has updated current and pending support disclosure requirements in its most recent Proposal & Award Policies and Procedures Guide (PAPPG) (NSF-22-1) and issued a table summarizing required disclosures. Although NIH and NSF maintain that their guidance constitutes

[5] NOT-OD-21-073, Upcoming Changes to the Biographical Sketch and Other Support Format Page for Due Dates on or After March 25, 2021; NOT-OD-21-110, Implementation of Changes to the Biographical Sketch and Other Support Format Page; and FAQs on Biosketches and Other Support and Foreign Components.
[6] NOT-OD-21-073.

"clarification" of existing requirements, the documents call for disclosure of items that are a departure from previously accepted standard practice, such as "in-kind" contributions of students working in labs, access to space or equipment, and collaborations. Institutions typically have established systems for collecting information on and vetting researchers' significant financial interests that may pose financial conflicts of interest (FCOI) based on agencies' long-standing FCOI regulations.[7] Unlike those FCOI regulations, however, recent support disclosure requirements have no minimum monetary thresholds, and institutions have been required to update their disclosure policies and processes to encompass these broad and fluid agency requirements. In addition, conflict of commitment is typically managed in a decentralized manner, at the department and school level, which adds an additional layer of complexity to institutional risk management.

COGR's paper "Principles for Evaluating Conflict of Commitment Concerns in Academic Research" ("Principles") provides a framework that institutions can use to evaluate their conflict of interest and conflict of commitment policies in light of recent agency guidance to address inappropriate foreign influence. The Principles recognize the value to institutions of permitting researchers to participate in outside activities, while acknowledging the need for "guardrails" to ensure transparency and protect both researcher and institution. These guardrails include processes for the disclosure and approval of potential conflicts of commitment; review of problematic clauses in contracts for external activities, including clauses prevalent in FGTP contracts; review and approval of consulting agreements; and consideration of researcher time spent on external activities. The Principles also consider the need for institutional communication and training to promote compliance, as well as sanctions for non-disclosure. Notably, NSPM-33 and the JCORE Guidance emphasize the need for agencies and institutions to increase awareness of research security concerns. In particular, Section 223 of the 2021 National Defense Authorization Act[8] limits enforcement against an institution for a covered researcher's failure to disclose required information if the institution made the researcher aware of the legislation's current and pending support disclosure requirements. This provision thus underscores the necessity for robust institutional training efforts.

Reporting Outcomes from Federal Research & Monitoring Efforts

As part of their investigative efforts into undue foreign influence, federal funding agencies have screened publications to identify:

- Funding sources that were not disclosed to the funding agency;
- Undisclosed affiliations with institutions other than the awardee; and
- Co-authors affiliated with/funded by non-U.S. institutions.

In cases where these issues were flagged, funding agencies often followed-up with the awardee institutions to determine if there were undisclosed significant financial interests, over-

[7] *See, e.g.,* 42 CFR 50, Subpart F.
[8] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Jan. 1, 2021)(see version entitled "Enrolled Bill").

commitments of time, undisclosed research support, scientific overlap between research projects, and, in NIH's case, undisclosed foreign components.

This scrutiny of external funding and collaborative relationships has led institutions to examine their policies and training on authorship considerations, as well as disclosure of institutional affiliations and external funding. Such training should warn researchers of the pitfalls of giving or accepting "gift" authorship, not only from a responsible and ethical conduct of research perspective, but also to avoid allegations of undisclosed support and/or foreign components. Professional associations and journals often have guidance about listing in publications author affiliations with institutions at which the research work was performed.[9] However, they do not generally delve into the potentially unethical listing of affiliations[10] (such as listing an institutional affiliation in exchange for payment), and institutions may want to consider how they will address such issues. Similarly, institutions should consider any laws[11] or funding agency policies regarding the listing of agency support in publications[12]. As with "gift" authorship, inappropriate acknowledgement of federal funding or failure to appropriately disclose sources of external funding may bring agency scrutiny.

Finally, in determining whether researchers are fully complying with institutional and agency disclosure requirements, institutions may want to consider monitoring strategies that include institutional review of publications and comparison of listed funding, affiliations and co-authors with disclosures made to the institution. It is unlikely that many, if any, institutions have the resources necessary to undertake blanket monitoring efforts for all researchers. Rather, institutions may want to consider a risk-based sampling approach.

Managing International Visitors and Students

The management of international employees, students, and visitors to campus cuts across several areas. For example, the application to support an H1-B visa has long included an attestation regarding the employee's access to export-controlled technology, and that if there is such access, appropriate licenses will be sought.[13] If foreign governments are paying for student tuition at U.S. universities at levels that exceed current reporting thresholds, such support must be disclosed as part of the Department of Education's Section 117 reporting. If students or post-doctoral trainees are supported by a foreign government or other external entity, some funding agencies require

[9] *See, e.g., Publication Manual of the American Psychological Association*, 7th ed. (2020); Elsevier Author Information Pack, p. 7 (July 15, 2021); *Science* Journals' editorial policies.
[10] *See*, Bachelet, V., *et. al.,* "Misrepresentation of institutional affiliations: The results from an exploratory case study of Chilean authors," 32 *Learned Publishing* 345-54 (Oct. 2019).
[11] *See*, "Stevens Amendment, §511, Pub. L. 101-166 (Nov. 21, 1989).
[12] *See,* NIH Grants Policy Statement, Section 4.2.1; NIH FAQs, Communicating and Publishing Federal Funding [e.g., FAQ#10 - "Generally, only grants that directly support the research activities contributing to the publication (e.g., authorship, consulting with authors, preparing manuscripts, and running analyses reported in the publication) and are within scope of the grant should be acknowledged in publications (see Public Access Reporting and Resource Sharing Blog 2016)"].
[13] https://www.nafsa.org/professional-resources/browse-by-interest/preparing-deemed-export-attestation-new-form-i-129

such support to be disclosed as "other" or "current and pending" support, particularly if the work they are doing intersects with grants to the U.S. research institution or investigator.

One area of potential risk is where the visitor has an affiliation with a restricted university or other restricted entity. Such restricted entities may be subject to stringent export control prohibitions, requiring technology control plans or other compliance strategies at the host institution. Research institutions may mitigate this risk by performing restricted party screenings on international visitors. This process may be straightforward in instances where the institution is supporting a visa application and screening can be integrated into the internal approval process. More intensive training and management is required to screen short-term visitors not sponsored by the institution, and in these cases a risk-based approach to securing access to research facilities may be warranted. It is important to screen not only the individual, but also their current affiliations as many universities in China, and similar countries of concern, may be either restricted parties or identified entities of concern. Research institutions should be aware of affiliations with these entities to make appropriate risk-based decisions about permitting the visit.

While restricted party screening is commonly used for foreign visitors accessing emerging technologies and research facilities, some institutions are expanding screening activities to encompass students as well. Decisions about screening students may raise sensitive issues including:

- Complying with non-discrimination policies;
- Communicating such screening to prospective students;
- Determining whether to screen only graduate students, or undergraduate students as well; and
- Addressing a past affiliation that is no longer active (e.g., a graduate student's undergraduate institution).

Institutions should consider the cost/benefit of such extensive screening practices as part of their risk-based decision making.

For international visitors engaging in research at the U.S. institution, it is important to have in place policies and procedures to protect institutional intellectual property. In the event there is a sponsored research agreement with the foreign entity supporting the visitor, this protection may come as a term in the agreement. In cases where there is no existing research agreement covering intellectual property, institutions may require visitors to sign access agreements and/or invention agreements prior to allowing them access to laboratories or technologies. In cases involving fundamental research, however, such agreements must carefully be considered to ensure that they do not compromise that research status.

Additional Security Considerations

Research institutions can protect their research environments by implementing appropriate cyber and physical security on their campuses. What these practices look like will depend on the nature of the activities in which the institution is engaged, starting with basic security precautions for

institutions operating in environments free from publication restrictions and with open participation for all individuals technically qualified to participate, and expanding to more extensive protections for institutions engaged in controlled research on behalf of the U.S. government. Regardless of which category an institution falls into, certain basic cybersecurity and physical security measures are essential to protecting the institution's assets and/or sensitive information and data.

Cybersecurity

Cybersecurity is an increasing focus for both institutions and policymakers at all levels. Higher education institutions are subject to numerous laws, regulations, and contractual obligations that specify requirements related to the appropriate management and protection of diverse data and information. For example, the White House recently issued an Executive Order on Improving the Nation's Cybersecurity.

Institutions need to be fully aware of these requirements and assure compliance. In the research context, attention must be paid to the security of a variety of resources from electronic lab notebooks to enterprise-wide research systems. Institutions also should remind individual researchers of the importance of ensuring the cybersecurity of systems they manage individually. A valuable resource in this area is EDUCAUSE's "Information Security Guide for Institutions of Higher Education." This Guide discusses a set of hot topics and includes a number of institutional case study submissions.

Recently, DOD issued contractual requirements pertaining to its Cybersecurity Maturity Model Certification (CMMC) framework. These are implemented through DFARS clauses 252.204-7012 and 7021. EDUCAUSE also recently developed a white paper on CMMC. The expectation is that the CMMC certification requirement will apply to all DOD contractors, with the certification level depending on the security requirements associated with the work performed for DOD.

The rollout of CMMC has been delayed for a variety of reasons, so the dates cited in the EDUCAUSE white paper are not necessarily current. Readers also are cautioned that there is a conceptual problem with the DFARS clauses as related to fundamental research. Fundamental research, by definition, does not include either Federal Contract Information or Controlled Unclassified Information, which triggers application of the CMMC. DOD is aware of this anomaly but has not yet found a solution.[14]

Physical Security

Physical security measures at research institutions vary with the sensitivity of the items/space to be secured. Unlike cybersecurity, where the regulatory environment is imposing increasing requirements, physical security at research institutions remains largely self-managed in accordance

[14] COGR and EDUCAUSE discussed the issue in a November 20, 2020 joint higher education association letter to DOD.

with local conditions and needs. It has become common for certain laboratory buildings and individual labs to have secure access, for safety and/or security reasons. Additionally, in the case of ongoing export-controlled equipment or research, the institution will implement a technology control plan that provides a written procedure for how the controlled items and research activities will be protected from unauthorized access and disclosure. Finally, institutional training for researchers often covers recommendations regarding security for activities such as tours of research spaces by outside groups.

Export Controls Compliance Programs

The U.S. export controls regulations are a series of individual regulations that work collectively to protect the nation's most valuable commodities and technologies. The Department of Commerce through the Export Administration Regulations (EAR), the Department of State through the International Traffic in Arms Regulations (ITAR), and the Department of Treasury through the Financial Asset Control Regulations (FACR) oversee the three main sets of export control regulations that apply to the university environment.

These regulations have received greater attention in recent years in part due to federal concerns that foreign national students and faculty may inappropriately export technologies and other sensitive information to their home countries. While the results of most university research are considered fundamental research that can be freely shared, there remains a perception that universities can, and should, do more to protect the pre-publication results of federally funded research through research security protocols, even when export controls are not applicable. Further, universities must take care to fully review contracts to identify "troublesome clauses" that can undermine the fundamental nature of the research and trigger the application of export control regulations (e.g., publication restrictions or restrictions on the citizenship of persons performing the research).

There has been recent legislative focus on the protection of emerging and foundational technologies. The Export Control Reform Act of 2018[15] requires the Department of Commerce to utilize an interagency process to define, identify, and control certain emerging and foundational technologies within the current export controls framework. Two separate Advance Notices of Proposed Rulemaking (ANPRM)[16] asked the community to comment on a definition and possible controls for each. COGR submitted two separate multi-association comment letters in response to these ANPRMs in January of 2019, and November of 2020, respectively. To date, the Department of Commerce Bureau of Industry and Security (BIS) has issued two federal register notices[17] announcing new controls on specific emerging technologies. BIS is expected to publish more controls in the coming years. It will be important for institutions to monitor these changes and understand the impact of any new technology controls on institutional research activities.

Federal enforcement agencies have consistently cited the presence of a well-maintained export controls compliance program as a mitigating factor in assessing penalties in cases involving an

[15] P.L. 115-232 (Aug. 13, 2018).
[16] 83 FR 58201 (Nov. 19, 2018) & 85 FR 52934 (Oct. 26, 2020).
[17] 85 FR 36483 (Jun. 17, 2020) & 85 FR 62583 (Oct. 5, 2020).

export controls violation. There are resources available to assist universities in creating an export controls compliance program. For example, the Department of Commerce, Department of State, and the Department of Treasury all have guidance on their websites on how to create and maintain a formal export controls compliance program. Another practical resource for universities continues to be the Department of Commerce's "Export Compliance Guidelines." In addition, associations like COGR and the Association of University Export Control Officers (AUECO), provide resources and/or hands-on training applicable to universities. Finally, the federal agencies named above (Commerce, State, Treasury) have also created and maintain export controls guidance and training.

Security Considerations Regarding Intellectual Property

Policymakers and law enforcement officials have expressed significant concerns about foreign theft or misappropriation of intellectual property (IP) generated by university research. The term tends to be loosely applied and expansive. Any creation of the mind can be considered as IP[18], though only some are subject to legal protection as property. For purposes of foreign influence concerns, it is important to distinguish among the different types of IP, as well as to distinguish between formal IP, subject to statutory protections, and the broader category of "intellectual capital" that does not fall into a formal IP class.

Formally Protectible Intellectual Property

Formally protectable IP such as patentable inventions tend to be well-protected by universities. Once a potentially patentable invention is reported to the technology transfer office (TTO), the disclosure is treated as confidential until a patent application is filed and any disclosure of enabling information by the TTO to an individual, company, or investor outside the institution occurs with a non-disclosure/confidentiality agreement in place. There is an exception for publication in a scientific journal, which is particularly important given the centrality of journal publication to the academic mission. Of course, having a non-disclosure agreement in place does not guarantee that an idea will be protected, but if the receiving party violates their secrecy obligations, the institution has standing to sue and can take legal action. If the TTO determines an invention is commercially significant and patent protection is warranted, the details are revealed by the inventor(s) in writing and/or verbally to a patent attorney (typically outside of the institution) who is bound by client confidentiality and subject to lawsuit or even penalties, including disbarment, if they do not maintain the information as secret and protected. While the process is not failsafe, it significantly reduces the potential for theft by any outside parties.

Software usually is protected by copyright, which is another form of protectible IP. Many universities do not register the copyright[19],as software often is released under "open source" licenses and the copyright is not enforced. Other forms of protectible IP relevant to universities

[18] *See,* World Intellectual Property Organization, "What is Intellectual Property?," (accessed July 2021).
[19] Note, however, that registration is not necessary for copyright protection. *See*, U.S. Copyright Office, FAQs, Copyright in General (accessed July 2021).

include IP related to chip designs. For more information on the technology transfer process see COGR's "Tutorial on Technology Transfer in U.S. Colleges and Universities."

If the TTO gets word of a potentially patentable invention not yet disclosed, the inventor might be contacted by the TTO and encouraged to avoid a public release of an enabling disclosure before the TTO has had a chance to evaluate and perhaps protect it. Constant education of faculty, researchers, and graduate students on IP and the patenting process remains essential. It also is critical for all institutions that receive federal research funding to have established policies and procedures that require inventors to assign ownership to the institution of any invention made using institutional funds or federal funds administered by the institution as required by federal regulations. Such policies help guard against researchers misappropriating the invention. For example, the University of Pennsylvania has a broad IP Participation Agreement that applies to employment by the university, participation in sponsored research, or use of funds, facilities, or other resources provided by the university. The Agreement assigns to the university all right, title, and interest to tangible and intangible research property, whether or not patentable, made in the course of employment at the university, from work directly related to professional or employment responsibilities at the university, from work carried out on university time, or at university expense, or with substantial use of university resources.[20]

Patenting and Licensing

Universities and other academic research institutions do not commercialize inventions by bringing them to the market themselves, but rather may license their discoveries to a company partner (a "licensee"), to further develop, test, manufacture, scale-up, and market the new product. Both licensor and licensee have an aligned interest in protecting an invention, and the IP claiming it, from unauthorized use and infringement. In addition, federally funded inventions sold in the U.S. usually are subject to a U.S. manufacturing requirement. To protect critical technologies in countries outside the U.S., a university patent holder can file patent applications in strategic or major market countries. Enforcement of patents in foreign countries is a complex topic beyond the scope of this paper, but, in brief, universities seek to protect patentable inventions domestically and internationally to the extent practical and necessary for commercialization. Finally, monitoring activities to ensure compliance with institutional IP requirements may include risk-based patent searches conducted by the TTO or legal counsel. Additional information on patenting and licensing can be found in COGR's publication "21 Questions and Answers About University Technology Transfer."

Unpublished Research Findings, Data and Materials

Additional concerns may relate to activities further upstream in the innovation process. A basic purpose of universities is to generate and disseminate knowledge. Open fundamental research is essential to this process. Unlike businesses, universities generally do not maintain trade secrets, as they want to share their knowledge to advance science. Even when information is ultimately

[20] For more information and FAQs on university and research institution intellectual property policies see World Intellectual Property Organization, "Frequently Asked Questions: IP Policies for Universities and Research Institutions."

shared, institutions remain concerned about protecting access to unpublished data and facilities to prevent "being scooped," and laboratory notebooks and biological or advanced materials may be of particular concern in this regard. Further, government investigative efforts have revealed that individuals who participate in malign FGTP programs may have contractually agreed to provide such unpublished data to an outside institution without the permission of the institution at which the work was generated.[21] Another consideration is implementation of steps to assure that peer reviewers and journal editors maintain the confidentiality of any proposed publication/manuscript/proposal.

Within the open academic environment, there are limited steps universities can take to protect innovative solutions, ideas for future research, and valuable knowledge that is not yet published, while also remaining true to the academic mission to disseminate and teach new knowledge. One strategy is to remind principal investigators that they should pre-approve team members' disclosure or sharing of pre-publication data outside the laboratory. Using a risk-based approach, institutions may want to implement additional screening for visiting researchers in labs in which there is concern about unpublished, innovative data. Such screening may gather additional information about the researcher's background, current appointments and affiliations, and purpose in visiting to determine if there are pertinent conflicts of interest or commitment, particularly contractual reporting obligations applicable to unpublished data and research findings. Additional physical and cybersecurity issues are addressed elsewhere in this paper and in other resources.

In some cases, institutions may take a completely different approach to the "protection" of research findings – the employment of an "open science" approach in which data is posted on open science platforms for peer review prior to formal publication. In this way, research integrity is promoted via full transparency and on-going review as the research progresses.

Startup Companies

Startup companies organized around IP created by academic research institutions present a valuable avenue to support regional economic development and product advancement, but they also are a particular area of concern with respect to inappropriate foreign influence or access. Institutional licensing of IP to such startups requires the conduct of appropriate due diligence including, for example, restricted party screening to understand who may be funding and controlling the startup company. Restricted party screening processes should be designed to capture all types of transactions with non-U.S. persons and entities, including licensing. In addition, for startups in high technology areas that may be of interest to foreign governments, other laws may come into play. In the U.S., controlling or certain non-controlling investments in U.S. businesses that produce, design, test, manufacture, fabricate, or develop one or more critical technologies in one of 27 identified industries – including aviation, defense, semiconductors, telecommunications, and biotechnology – are subject to a mandatory filing with the Committee on Foreign Investment in the U.S. (CFIUS) which provides an added layer of scrutiny and diligence. Universities working with startups should be aware of the CFIUS regulations.

[21] *See*, M. Lauer, "Addressing Foreign Influence and Associated Risks to the Integrity of Biomedical Research, and How You Can Help," NIH Extramural Nexus (July 8, 2020).

Startups also may raise concerns about conflicts of interest and conflicts of commitment. Many universities have Startup Guides. Two in particular that provide valuable information about these and other considerations with startups are Johns Hopkins University's "Startup Guide - A Guide to Technology Licensing and University Startups" and Stanford University's "Start-Up Guide."

Reporting of Gifts to Institutions: Department of Education Section 117 Reporting

The Higher Education Act of 1965[22] included the Section 117 requirement that academic institutions receiving Title IV funding report every six months to the Department of Education (ED) foreign gifts and contracts aggregating to $250,000 in a calendar year (July 31 and January 31 reporting deadlines). Prior to 2019, ED provided two "Dear Colleague" letters (1995 and 2004) as the only interpretive guidance to academic institutions on how to comply. In February 2019, the Senate Permanent Subcommittee on Investigations held a hearing on "China's Impact on the U.S. Education System" which featured testimony from Deputy Secretary of Education Mitchell M. Zais regarding Sec. 117. Following this testimony, ED became actively engaged in Section 117 compliance, launching investigations of noncompliance at several institutions.[23] Additionally in 2019, ED issued an Information Collection Request[24] (ICR) expanding the reporting requirements to include additional information. Importantly, the ICR and additional interpretive guidance impose criminal as well as civil penalties for noncompliance.

In 2020, ED launched a new online reporting portal to collect the required information from academic institutions. The portal requires that each gift or contract be reported individually (it does not include at this time a bulk upload capability). In addition to reporting the dollar value of the gift or contract, the identity of the donor/sponsor, as well as any restrictions on the gift or contract must be reported. Information reported to ED is made publicly available at an ED website. The American Council on Education has been at the forefront of advocacy for academic institutions on Section 117.

It should be noted that legislation currently under consideration will change the reporting threshold from $250,000 to $50,000 per calendar year. Additionally, there will be a record retention obligation for the contract or gift agreement. Finally, institutions should be aware of state reporting requirements related to foreign gifts and contracts that may apply.

Governance

With the ever-increasing focus on the complex science and security issues outlined above, institutions also must consider the administrative structure that they will use to operationalize their research security processes. Security is a cross-cutting issue that requires communication, information sharing, and collaboration among a large swath of institutional administrative units including units that handle conflict of interest and commitment sponsored projects; technology transfer; information technology and security; international students and scholars, and others.

[22] P.L. 89-329 (Nov. 18, 1965).
[23] *See,* Dept. of Education, Section 117 of the Higher Education Act of 1965 webpage. .
[24] *Id*.

Accordingly, many institutions have determined that an interdisciplinary task force or work group is necessary to respond effectively to the various requirements and concerns.

In addition, Section 4(g) of NSPM-33 states that funding agencies shall "require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program." Similarly, the second recommendation in the JCORE Guidance states that organizations "should develop written security implementation plans" and "designate a chief research security officer or equivalent to oversee research security management." In determining where these functions will be housed, institutions must consider whether research security functions and personnel should be incorporated into current units, and if so, which units, or whether a new unit should be created. If a new research security unit is created, institutions must consider how it will integrate with existing units that have responsibilities that may touch on research security and integrity (e.g., conflicts of interest office, sponsored programs office, research integrity office, visa office, etc.) In all cases, institutions must consider how information pertinent to research security and scientific integrity will be appropriately shared across units.

To make appropriate risk-based decisions in this arena, institutions will need to consider the nature of their own research portfolios, including, among other factors, whether they work on export controlled or restricted research; the volume of cross-border collaborations; and the volume of visitors to campus. By adopting this risk-based approach, institutions can better strike the correct balance between implementing research security practices that are appropriate to the institution's unique circumstances and continuing to support and foster the international scientific collaborations, research, and teaching that lie at the heart of the academic mission and are crucial to the success of both U.S. and global scientific progress.

Cost Implications to Institutions

Responding to agency mandates concerning research security, as well as implementing the JCORE Guidance, will necessarily involve additional institutional costs. Although costs will vary widely across institutions based on their individual research portfolios, common components such as additional cybersecurity measures and ensuring that institutional systems can "talk to each other" to improve disclosure accuracy are "big-ticket" items. To date, however, none of the legislation, guidance, or policies issued by the federal government in this arena have included provisions to supplement institutional funding.

The annual Higher Education Research & Development Expenditures (HERD) Survey, conducted by the National Science Foundation, National Center for Science and Engineering Statistics (NCSES), provides important data on the ever-expanding role research institutions play in supporting the research enterprise—while also providing some clues to how unfunded mandates affect the financial health of research institutions. According to the most recent 2019 InfoBrief released by the NCSES:

> Federally funded R&D at universities increased 6.3% to $44.5 billion in FY 2019. This total was $2.6 billion greater than the FY 2018 total and is the largest percentage increase since

> FYs 2010–11. ***The share of higher education R&D supported by the federal government remained about 53% for the third consecutive year after declining gradually from 62% in FY 2011*** *[emphasis added]* … Institutions' own funding, which rose $900 million (4.4%) from FY 2018 to FY 2019, accounted for the second largest share of R&D funding (25%).

The federal government is the primary funder of the research enterprise providing $44.5 billion (53%) in 2019. However, institutional funding of research now stands at an all-time high of $21.2 billion (25%). Further, NCSES Table 16 shows that of the $21.2 billion of institutional funding, $5.5 billion represents institution-subsidized unrecovered indirect costs—normally caused by funder-imposed restrictions on indirect cost recovery. Not included in the $5.5 billion is the additional subsidy incurred by research universities due to the 26% administrative limitation, and some estimates suggest that this adds at least an additional $1 billion to the institutional subsidy. This institutional subsidy, which includes both funder-imposed restrictions and the 26% cap effect, in the context of the federal government's call for additional, wide-ranging research security requirements, is another example of regulatory creep. This phenomenon occurs when new regulations (or in some cases "guidance") issued by funding and oversight agencies (at times driven by statutory requirements and at other times issued by agency proclamation) add more and more administrative burden to research institutions without providing associated funding, ultimately, increasing the institutional subsidy. While both institutions and funding agencies agree on the need for, and public value of, a risk-based approach to research security, requiring institutions to fully bear the associated cost poses the risk of creating an administratively burdensome and expensive unfunded mandate.

Conclusion

Over the past few years, academic research institutions have become increasingly attuned to research security considerations, and Director Wray's 2018 description of "naivete" in this area does not currently hold true. Today, institutions engage in a continued assessment of the security and integrity of their research enterprise, and they have taken significant steps toward mitigation while maintaining fidelity to the critical academic values of openness and dissemination. Although each institution's journey along this path differs based on its individual circumstances, risk assessment, and timeline, institutions will need to consider the research security facets outlined in this paper as part of the process of developing a robust and appropriately focused research security program. Institutions also must recognize that the successful development of such a security program is dependent not only on assessing risk, but also adhering to the JCORE Guidance's mandate to pursue a "balanced" approach that "recognize[s] the benefits of open, international collaboration." It is only through such a balanced risk/benefit analysis that academic institutions can develop appropriate research security measures while still achieving their primary goal of widespread education and knowledge dissemination.