University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus

Updated May 2020

AAU and APLU have previously identified and shared effective practices universities are employing to ensure the security of research, protect against intellectual property theft and academic espionage, and prevent actions or activities by foreign governments and/or other entities that seek to exert undue foreign government influence or infringe on core academic values (e.g. free speech, scientific integrity, etc.).

The associations first surveyed universities regarding actions they have taken to address concerns about research security threats and undue foreign influence on campus in fall 2018. After completing the survey in April 2019, we released a comprehensive summary of examples of effective policies, practices, tools, and resources universities have had in place or are newly employing to address ongoing and emerging foreign security threats.

In the fall of 2019, the associations conducted a follow-up survey. The following incorporates new and existing activities universities are pursuing, according to the recent survey collection. We encourage all universities to review these examples and to consider implementing practices that might prove effective on their own campuses to protect against research security threats and undue foreign government influence. The Council on Governmental Relations (COGR) also assisted in review of this document.

AWARENESS BUILDING AND COMMUNICATIONS

- ***Distribution of campus-wide communications.*** Institutions have distributed communications to faculty, staff, post-doctoral associates, and graduate research assistants to increase awareness and provide information on undue foreign government influence. These communications often include information on: actions researchers can take to mitigate risks; whom at their institution to contact for assistance or to address questions; and reminders of existing reporting, disclosure, and export and other security control requirements and responsibilities under federal and institutional rules and policies.
- ***Publication of security newsletters and presentations.*** Institutions have published and distributed security newsletters covering foreign threats to intellectual property and international travel preparation. Campus-based facility security and export control officers also have reported providing regular security briefings to university leadership and working to facilitate such briefings with their regional FBI offices, given heightened concerns about foreign threats.
- ***Creation of comprehensive and publicly available websites.*** Institutions have created and made public websites with links and information on a wide range of topics, including international research engagements, international research and global collaboration, undue foreign government influence, and risk mitigation. Websites also serve as a "one-stop" reference points to access relevant university policies and practices, university communications and guidance, and agency information, policies, and requirements.
- ***Regular discussions at university leadership and faculty meetings.*** Institutions have regular discussions across campus groups, including faculty, deans, department chairs, and senior administrators on undue foreign government influence issues. Discussions also take place on faculty listservs regarding issues to consider when participating in international engagements.

COORDINATION

- ***Formation of campus-wide working groups and task forces.*** Institutions have continued to refine campus-wide working groups and task forces, with some increasing representation at both the leadership and operational levels, including senior administrators and faculty. These cross-campus working groups discuss, develop, and implement strategies to better coordinate and address concerns regarding security threats and undue foreign government interference. These groups may also discuss pressing global matters regarding the health, safety, and security of faculty, students, and staff abroad as well as any foreign engagements/decisions/activities abroad that might impact the university as a whole.
- ***Coordination of risk assessment.*** Institutions have created campus-wide committees of research leaders, compliance officers, and security personnel who develop risk inventories, assess areas of research and scholarship that could be at risk of undue foreign government influence, and provide potential security solutions. These assessments are done in consultation with local Federal Bureau of Investigation (FBI) field offices or other national security experts.
- ***Formation of international activities, forums, and compliance coordination offices***. Institutions have organized new offices or shared workflow processes to better coordinate, oversee, and continually review their activities involving international partnerships, foreign engagements, and compliance requirements. These offices oversee functions ranging from export controls, to review of foreign visitors, to issues associated with international students and scholars. Some of these offices have continued to expand strategic planning, advice, and assistance to administrators, faculty, and staff on international operations, security, and other high-risk activities through both one-on-one consultations and larger campus forums and events.

TRAINING OF FACULTY AND STUDENTS

- ***Modification of Responsible Conduct of Research (RCR) training to inform students and faculty of foreign threats and federal export control, disclosure, and reporting requirements.*** Institutions have incorporated modules on export-controlled research, protection of intellectual property, preservation of scientific integrity, ethical behavior in conducting federally-funded research, agency reporting and disclosure requirements, and processes for reporting suspicious behavior into RCR training for students and faculty. These efforts often include providing information on technical areas of specific interest to U.S. government competitors and are being conducted in the context of broader university initiatives to educate and raise awareness among faculty and students concerning current foreign government threats and how to take protective measures in response. Some institutions are now offering special online training modules on complex ethical decision making, for-credit RCR coursework for graduate students, and competency certificate programs for faculty and staff to understand university policies and resources. Additionally, some institutions are providing additional training to researchers whose research has been identified as potentially more vulnerable to security breaches or to undue foreign government influence.
- ***Creation of webpages and training materials for faculty and staff.*** Institutions have created comprehensive websites for faculty and staff to have easy access to institutional and federal agency requirements regarding disclosures of all outside research funding sources and compliance requirements placed on federal research grants.

- ***Increased collaboration with federal security agencies.*** Institutions have worked with federal security agencies, including the FBI, Defense Counterintelligence and Security Agency (DCSA), and the Department of Homeland Security (DHS) to develop training materials for campus leaders and faculty on research and cyber security threats. Agencies are often invited to campus to provide direct briefings and trainings to both faculty and administrators.

REGULAR INTERACTIONS WITH FEDERAL SECURITY AND INTELLIGENCE AGENCIES

- ***Establishment of a clear point of contact (POC) and strong relationship with regional federal security officials.*** Institutions have developed much stronger relationships and are regularly interacting with local and regional officials from the FBI, ICE, Defense Security Service (DSS), and other federal law enforcement and security organizations. This includes senior university administrator participation in classified briefings. Many institutions have established a primary campus point of contact for these agencies, with whom they may interact when they have identified specific issues or real or potential threats to campus or if they have concerns about the activities of specific faculty and/or students. Institutions use the FBI as a valuable resource to consult in the screening of foreign visitors, provide security updates, and offer training opportunities (such as the FBI Citizens Academy, which helps to explain how the FBI operates). In addition, institutions have partnered with local officials to provide a venue for collaborative activities, such as hosting meetings on campus for leadership and attending regional conferences.

PROTECTION OF DATA AND CYBERSECURITY

- ***Enhancement of data handling and management.*** Institutions have updated training, tools, policies, and governance for handling data and developed comprehensive approaches for storing, protecting, and ensuring the appropriate use of different types of data. In particular, institutions have identified appropriate protections for sensitive data in grants and contracts to ensure compliance with NIST SP 800-171 Rev. 1, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." Institutions regularly include an information technology Memorandums of Understanding (MOUs) among the standard contract documents used with third-party service providers such as vendors that provide hosted technology solutions and stipulates that data will be hosted in the United States unless approved by the Chief Information Officer. Before purchasing software, institutions screen denied and restricted parties' databases (Visual Compliance or Amber Road). Data security review has also been incorporated into the Institutional Review Board (IRB) review process, allowing for review and identification of where data is stored and who owns data.
- ***Improved data security measures.*** Institutions have taken measures to improve data security, internal breach prevention, and incident response processes. This includes bolstering network perimeter security and conducting enhanced monitoring of network traffic. Institutions are using encryption, multi-factor authentication, and virus scanning to protect data. They also are developing new processes for monitoring systems and networks for intrusions and reporting suspected data breaches. Institutions have deployed Security Information and Event Management (SIEM) systems to better detect and respond to cyberattacks as well as creating cybersecurity incident response plans to provide guidance on how to identify, report, and mitigate security incidents.
- ***Development and use of coordinated approaches for cyber threat notification.*** Institutions have joined the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC), which

monitors the threat landscape and seeks to enhance operational security and mitigate risk at higher education institutions. REN-ISAC works with trusted third parties to notify its 627 institutional members of infected hosts and suspicious network traffic. Institutions also have joined the Omni Security Operations Center (OmniSOC), an initiative aimed at reducing cybersecurity threats and serving as a cybersecurity operations center that can be shared among multiple institutions. OmniSOC analyzes data for potential threats and notifies members when incidents require further action.

- ***Increased training and faculty support.*** Universities have expanded their training opportunities to include targeted outreach to faculty and staff on special information technology needs. Universities regularly host speakers on cybersecurity threats and have created one-stop, self-service, online resources for researchers to secure data and ensure compliance with rules and regulations.

PROTECTION OF INTELLECTUAL PROPERTY AND USE OF TECHNOLOGY CONTROL PLANS

- ***Development and use of faculty disclosure requirements for intellectual property (IP) protection.*** Institutions routinely require faculty disclosure of intellectual property with commercialization potential, with the intent of ensuring that such IP is secured by quickly applying for the appropriate patent protection. Institutions also protect and restrict access to specific information on university invention disclosures, patent applications, and license agreements.
- ***Use of Technology Control Plans (TCPs) and non-disclosure agreements.*** Institutions regularly establish TCPs and other risk-mitigation initiatives to ensure the security of research and protection of intellectual property and to maintain compliance with federal regulations, laws, and contract directives. In instances where proprietary research is being conducted, institutions regularly make use of non-disclosure agreements.

REVIEW OF COLLABORATIONS, CONTRACTS, AND FOREIGN GIFTS

- ***Development of risk criteria and use of comprehensive processes for review of grants, contracts, and foreign gifts.*** Institutions have established extensive routing and screening systems for agreements and awards involving foreign support. This involves scanning agreements for foreign engagement, export controls, grant terms and conditions, and the potential receipt or generation of sensitive data or information. Institutions use risk criteria to assess agreements involving high-risk activities or countries of concern and, when deemed appropriate, help guide institutions to conduct additional in-depth reviews of international sponsorship requirements, export control risks, and information security controls. For those that require additional screening, this has sometimes resulted in revision of specific proposed agreement terms and conditions or a decision to not enter an agreement. Institutions have also greatly stepped up their efforts to ensure comprehensive collection and reporting of foreign gifts and contracts to the Department of Education to ensure full compliance with the requirements under Section 117 of the Higher Education Act. Research offices and general counsels often evaluate reported gifts.
- ***Development and use of templates to mitigate risks and protect against foreign threats.*** Institutions have developed templates to guide faculty and staff as they review and consider entering into partnerships and/or agreements with foreign entities. These templates often include prompts with the intent of mitigating potential risks; protecting core academic values such as free speech, academic freedom, reciprocity, and other ethical considerations; and ensuring compliance with export-control laws and other federal requirements. Some institutions have also adopted a decision matrix for international agreements to provide better guidance for faculty seeking to enter into such agreements.

- ***Use of restricted or denied party screening techniques and tools.*** Institutions have expanded their techniques for screening foreign sponsors and collaborators and partnerships with foreign universities – including visitors, visiting scholars, and employees and students on non-immigrant visas – to ensure compliance with federal export control requirements and restricted entities lists. Many institutions use software solutions, such as Visual Compliance or Amber Road; and enterprise resource planning (ERP) software, which searches numerous continually updated security red-flag and export control lists, to screen for restricted or denied parties. If an individual or entity is present on a restricted, denied, debarred, designated, or blocked party list, they may be prohibited from entering into new partnerships or otherwise doing business with or providing services to the institution and/or may be restricted in their access to specific facilities or information.

REVIEWING, UPDATING, AND ENFORCING CONFLICT OF INTEREST POLICIES

- ***Development and use of Conflict of Interest (COI) and Conflict of Commitment (COC) policies.*** Institutions continue to use and update existing COI reporting requirements to identify faculty who have foreign financial interests, including affiliations with foreign institutions of higher education. Institutions also continue to expand their existing COI policies by developing complementary COC polices. These policies are being updated to more clearly identify foreign affiliations, relationships, and financial interests which may conflict with the faculty member's responsibilities to their home institution or otherwise raise concerns. This includes adding more targeted questions about affiliations with government-sponsored talent recruitment programs; titled positions, recognitions, and/or status with an institution outside the United States; paid and/or unpaid international collaborations; and service as a principal investigator outside the institution. Updated policies also include language that specifically prohibits individuals from engaging in foreign licensing and disclosure of IP without following appropriate university guidelines. Many institutions have voluntarily notified federal funding agencies when discrepancies have been found.
- ***Development of infrastructure for information collection and tools to support disclosure reporting.*** Institutions have built electronic systems to track and maintain records of disclosure reports in addition to building staff capacity to more closely monitor reported information. Institutions have also increased coordination, particularly with the export control office, to review reports concerning faculty foreign activities and actively seek opportunities to provide needed research security training to faculty, staff, postdoctoral associates, and graduate research assistants. Some institutions have also developed and shared scenarios, case examples, and FAQs to aid those who submit disclosures as well as checklists for chairs, deans, and other supervisors to consider during disclosure review to determine if greater review of a disclosed activity may be necessary.

FOREIGN TRAVEL SAFEGUARDS AND PROTECTIONS

- ***Development of international travel policies.*** Institutions have developed and are updating international travel policies for faculty and staff traveling abroad as part of a university-sponsored or supported international travel program to include pre-registration of foreign travel. Some institutions provide security briefings for individuals traveling internationally on university business, teaching, research, or travel abroad and tailored one-on-one briefings as needed for destinations considered high-risk.

- ***Deployment of faculty foreign travel review and assistance.*** Institutions have created programs, often through their export control or research compliance offices, for reviewing faculty and administrators' travel for export compliance, software use restrictions, and other safety and security concerns. This includes cleaning laptops, iPads, smartphones, and other electronic devices to make sure they are protected from cybertheft before, during, and after travel in specific countries. Institutions with these programs will often provide blank, secure loaner laptops to researchers traveling abroad and encourage faculty not to cross international borders with devices containing research data. The U15 Group of Canadian Research Universities also produced a paper, "Travel Security Guide for University Researchers and Staff," which details risk-mitigation strategies that faculty and staff should review before traveling abroad (including people-to-people connections, physical intrusions, and cyber intrusions).

INTERNATIONAL VISITORS TO CAMPUS

- ***Development and use of requirements for vetting and securely hosting foreign visitors while on campus.*** Institutions have developed policies requiring faculty to alert university officials, often through their export control, research compliance, or international affairs offices, when they plan to have foreign visitors come to visit campus and/or tour their laboratories. The hosting faculty member may be required to fill out a brief questionnaire and/or form for each visitor. Some institutions use software solutions such as Visual Compliance or Amber Road, which search numerous continually updated restricted parties lists, to screen for restricted or denied parties. Other institutions have implemented measures for securely hosting and escorting foreign visitors and avoiding unauthorized information gathering. Some institutions are also now choosing to screen all visiting foreign scholars, which previously may have been limited to scholars in visa categories requiring screening under export control regulations.
- ***Implementation of visitation control plans and visiting scholar handbooks.*** Some institutions and departments have created plans to detail specific measures the host will take to prevent unauthorized access to export-controlled data and areas where export-controlled research is performed. Submitted plans often include a list of visitors, who they meet with, the duration and campus location of their visit, and the purpose of their visit. Institutions have also provided detailed handbooks with guidance on how to successfully invite and host a visiting student researcher or a visiting scholar on campus including details on how visitors should be onboarded.
- ***Development of resource documents on foreign engagements and visitors to campus***. The Academic Security and Counter Exploitation Working Group (ASCE) produced a paper, "Steps and Considerations for Effective Foreign Visitor Review Process in an Academic Environment." The paper suggests a checklist for foreign visitor review processes including: determining the level of risk proposed by the visitor, reviewing the visitors background and reason for visit, preparing an official university invitation, managing the onboarding process and oversight while visitor is on campus, and completing the departure process for the foreign visitor. ASCE also includes a list of suggested interview questions that institutions could use for foreign visitors. COGR produced a "Framework for Review of Global Engagements in Academic Research" to provide an underlying structure to support an institution's analysis of global research engagements, assess potential risks, and develop strategies for mitigation. The U15 Group of Canadian Research Universities also developed a paper, "Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects: A Tool for University Researchers," to assist with identifying and mitigating risks with research collaborations and projects, and provides a checklist for building a strong project team, assessing non-academic partners, and reviewing use of research findings.

The Australian Group of 8 has also produced "Guidelines to Counter Foreign Interference in the Australian University Sector" to help manage and engage with risk to deepen resilience against foreign interference in the university sector.

EXPORT CONTROL COMPLIANCE

- ***Use and strengthening of policies and programs to ensure full compliance with federal export control requirements.*** Institutions have in place clear, visible, and comprehensive policies regarding whether and how they will undertake export-controlled research activities. This includes applying for export control licenses when required and creating TCPs to protect technology from unauthorized access when export-controlled technologies are involved and/or classified work is being conducted.
- ***Employing university staff with specific export control compliance expertise.*** Most AAU and APLU institutions have one or more staff members with specific responsibility for ensuring compliance with export controls. Many of these individuals belong to the Association of University Export Control Officers (AUECO), a national association of more than 270 university export control officers, whose mission is aimed at exchanging information and sharing knowledge and effective university policies and procedures to advance university compliance with U.S. export, import, and trade sanctions laws and regulations. Institutions conducting classified research also have specially trained Facility Security Officers (FSOs), who oversee security specific to this research.