Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus

Updated - April 22, 2019

AAU and APLU are identifying and sharing practices that 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 influence or which infringe on core academic values (e.g. free speech, scientific integrity, etc.).

The associations recently conducted a survey asking campus representatives to provide examples of effective policies, practices, tools, and resources they are using and which other campuses may benefit from learning about as our universities collectively work to address ongoing and emerging foreign security threats. The following is a sample of some of the activities being pursued by universities, both existing activities in response to federal requirements and emerging activities in response to recent security concerns, in over 140 examples submitted by 39 institutions. We encourage all universities to review these examples and to consider implementing many of these practices on their own campuses as deemed appropriate to protect against security threats and undue foreign influence. Additional support collecting and summarizing these examples was provided by the American Council on Education (ACE) and the Council on Governmental Relations (COGR).

AWARENESS BUILDING AND COMMUNICATIONS

- ***Distribution of campus-wide letters on safety and security to increase faculty awareness and remind the campus community of existing reporting requirements.*** Institutions have distributed letters to their faculty to increase awareness of systematic programs of foreign influence and how such programs pose risks to core scientific and academic values and threaten research integrity. These letters often include information reminding faculty of their existing reporting and disclosure requirements under federal and institutional policies.
- ***Publication of security newsletters and presentations.*** Institutions have published and distributed security newsletters covering topics including foreign threats to intellectual property and international travel preparation. Campus-based facility security and export control officers also have reported providing additional security briefings to university leadership and working to facilitate such briefings with their regional FBI offices given heightened concerns about foreign threats.

COORDINATION

- ***Formation of high-level working groups and task forces.*** Institutions have formed cross-campus working groups and task forces consisting of senior administrators and faculty to discuss, develop, and implement strategies to better coordinate and address concerns regarding security threats and undue foreign influence.
- ***Formation of international activities 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 also provide strategic planning, advice, and assistance to administrators, faculty, and staff on international operations, security, and other high-risk activities.

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 untoward actors and are being conducted in the context of broader university initiatives to educate and raise awareness among faculty and students concerning current foreign threats and how to take protective measures in response.

REVIEW OF FOREIGN GIFTS, GRANTS, CONTRACTS, AND COLLABORATIONS

- ***Development and use of comprehensive processes for review of foreign gifts, grants, and contracts.*** 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 and routing documents as needed for in-depth review of international sponsorship requirements, export control risks, and information security controls.
- ***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, and ensuring compliance with export control laws and other federal requirements.
- ***Use of restricted or denied party screening techniques and tools.*** Institutions are expanding their techniques for screening foreign sponsors and collaborators, including visitors, visiting scholars, and employees on non-immigrant visas, to ensure compliance with federal export control requirements and restricted entities lists. Many institutions are using software solutions such as Visual Compliance, which searches numerous continually-updated restricted parties 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 doing business with or providing services to the institution or may receive restricted access to specific facilities or information.

REVIEW OF FACULTY FOREIGN FINANCIAL INTERESTS AND AFFILIATIONS

- ***Development and use of Conflict of Interest and Conflict of Commitment policies.*** Institutions are using existing Conflict of Interest (COI) reporting requirements to identify faculty who have foreign financial interests, including affiliations with foreign institutions of higher education. Institutions have expanded their existing COI policies by developing complimentary Conflict of Commitment polices. These policies seek to identify foreign affiliations, relationships, and financial interests which may conflict with the faculty member's responsibilities to their home institution or otherwise raise concerns. Institutions also have enhanced their screening of COI disclosures for international activity.

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."
- ***Improved data security measures.*** Institutions have taken measures to improve data security and internal breach prevention and incident response processes. This includes bolstering network perimeter security and conducing enhanced monitoring of network traffic. Institutions are using encryption, multi-factor authentication, and virus scanning to protect data and are developing new processes for monitoring systems and networks for intrusions and reporting suspected data breaches.
- ***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 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.

PROTECTION OF INTELLECTUAL PROPERTY AND USE OF TECHNOLOGY CONTROL PLANS

- ***Development and use of faculty disclosure requirements for intellectual property protection.*** Institutions routinely require disclosure of intellectual property with commercialization potential by faculty, 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.

REGULAR INTERACTIONS WITH FEDERAL SECURITY AND INTELLEGENCE AGENCIES

- ***Establishment of a clear 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 organizations. This includes participation by senior university administrators in classified briefings. Institutions have established a primary campus point of contact for these agencies, with whom they may interact when they have identified issues or threats to campus or if they have concerns about the activities of specific faculty and/or students. Institutions described utilizing the FBI as a resource for consultation regarding the screening of foreign visitors and collaborators and as a source of security updates.

FOREIGN TRAVEL SAFEGUARDS AND PROTECTIONS

- ***Deployment of faculty foreign travel review and assistance.*** Institutions have created programs, often through their export control or research compliance offices, for reviewing travel by faculty and administrators 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 cyber theft 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. Some institutions also provide security briefings for individuals traveling internationally on university business and tailored one-on-one briefings as needed for destinations considered high-risk.

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, which searches 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.

EXPORT CONTROL COMPLIANCE

- ***Use and strengthening of policies and programs to ensure full compliance with federal export control requirements.*** Institutions have in place clear 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 Technology Control Plans (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 Compliance Officers (AUECO), a national association 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.