



International Advocacy Coordinating Committee and Public Policy Town Hall

**Craig Lindwarm & Debbie Altenburg
APLU Government Affairs**

Science and Security Overview

- National security is core to the government-university research partnership.
- Security controls must be carefully balanced with the need to ensure the free flow of fundamental scientific information and talent.
- Universities take seriously national security threats posed by international actors.

APLU/AAU Best Practices Survey

- APLU and AAU are identifying and sharing practices that universities are employing to ensure the security of research, protect against IP theft and academic espionage, and prevent actions or activities by foreign governments that seek to exert undue foreign influence or infringe on core academic values
 - December 2018 survey with 142 responses from 39 institutions
 - **April 2019 memo to institutions encouraging all universities to consider implementing practices on campus as deemed appropriate**

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 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.

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 to screen for restricted or denied parties. Other institutions have implemented measures for securely hosting and escorting foreign visitors and avoiding unauthorized information gathering.

Regular Interactions with Federal Security and Intelligence 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.

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 conducting 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.

Protection of Data and Cybersecurity (continued)

- ***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 629 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.

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 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.

Science and Security

Federal Agency Update

National Institutes of Health

- NIH convened a working group to address foreign influence and research integrity. Its final report on December 2018. Five APLU presidents were members of the working group.
- Subsequent investigations by NIH has identified
 - Undisclosed foreign financial conflicts
 - Failure to disclose financial support
 - Undisclosed conflicts of commitment
 - Failure to disclose affiliations and positions
 - Peer review violations
 - Inappropriately transmitting information
- NIH issued a notice on July 10 reminding grantees of responsibilities with regard to disclosing foreign activities that may interact with NIH funded activities.

National Science Foundation

- On July 11 NSF Director France Córdoba issued a Dear Colleague Letter on research protection.
- The letter recognizes the great strength of the U.S. research and engineering enterprise is the diversity of talent- both domestic and international.
- However it goes on to say that the science and engineering enterprise is put at risk when “another government endeavors to benefit from the global research ecosystem without upholding the values of openness, transparency, and reciprocal collaboration.”
- NSF will be implementing an electronic portal for all grantees to submit biographical sketches, including disclosure of all appointments and support starting January 2020.

Department of Energy

- In June, the Department of Energy issued a directive prohibiting DOE employees and DOE contractor employees, “from the unauthorized transfer of scientific and technical information to foreign government entities through their participation in foreign government talent recruitment programs of countries designated by DOE as a foreign country of risk.” (China, Russia, North Korea, and Iran)
- DOE is also in the process of working on a “threat matrix” the national labs will use to evaluate future research partnerships with individuals or institutions in these nations.

Department of Defense

- Both the House and Senate have passed their versions of the National Defense Authorization (NDAA) bills.
- Both bills contain provisions that would impact research security at academic institutions.
- APLU has endorsed an amendment by Rep. Mikie Sherrill (D-NJ) based on her bill “[Securing American Science and Technology Act.](#)” The bill is the result of efforts to proactively and constructively develop ideas to protect the U.S. scientific enterprise from foreign interference, cyberattacks, theft, and espionage.
- The 2019 NDAA contained a prohibition on institutions with Confucius Institutes from participating in DOD language instruction programs, although the prohibition would allow the DOD to waive the prohibition at its discretion. DOD has declined to issue any waivers.

Department of Education

- The Department of Education has begun institution investigations in to compliance on Section 117 of the Higher Education Act, which requires institutions who receive Title IV federal student aid funds to report to the department gifts received from foreign sources.
- Members of Congress in both the House and Senate are currently looking at potentially lowering the reporting threshold from its current level of \$250,000

What's Next?

- APLU will continue to:
 - Share the benefits of international collaborations
 - Emphasize openness, academic freedom, and the transmission of knowledge
 - Engage with campus leadership, key policymakers and federal security and research agencies to address undue foreign interference in research performed at U.S. universities
 - Welcome continued engagement and feedback from member institutions
 - Explore the benefit of additional surveys, information gathering on campus activities, and effective practices

DACA and Dreamer Updates

- It's come to this. Action in the U.S. Supreme Court
- Can Congress ever solve this problem?



Trump Admin. & Intl. Students

- Processing Delays
- Optional Practical Training (OPT)
- Unlawful Presence
- Duration of Status
- APLU engagement w/ administration

High-Skilled Immigration Reform

- Employment/“Merit-based” vs. family-based/“chain”
- A moving bill? Fairness for High-Skilled Immigrants Act
- Change in political dynamics on the Hill: The old high-skilled coalitions are gone

Budget & Appropriations

- Budget Control Act of 2011: Please, let's be done with it.
- Status of FY 2020 Appropriations
- Yet Another Potential Fiscal Cliff



QUESTIONS? LET'S CHAT

Craig Lindwarm

Vice President, Congressional & Governmental Affairs

APLU

clindwarm@aplu.org

[@APLU_GovAffairs](#) [@craiglindwarm](#)

Debbie Altenburg

Assistant Vice President, Research Advocacy and Policy

APLU

daltenburg@aplu.org

[@APLU_GovAffairs](#)

