ABOUT: In its fourth year, this seminar brings together experts from academia, the private, and federal agencies to examine, promote awareness of, and counter the threat posed by foreign influence and theft of academic research.

NOTE: March 2-4 are open to any university. March 5-6 are intended for universities participating in the National Industrial Security Program.

KEYNOTE SPEAKERS

Mr. David Bowdich  
Deputy Director, Federal Bureau of Investigation

Mr. John Demers  
Assistant Attorney General for National Security

Kelvin K. Droegemeier, Ph.D.  
Director, White House Office of Science and Technology Policy

Mr. William Evanina  
Director, National Counterintelligence and Security Center

Maj. Gen. Thomas Murphy  
Director, Protecting Critical Technology Task Force, Office of the Secretary of Defense

SEMINAR TRACKS

The ASCE Annual Seminar features tracks for security and compliance, cyber security, and executive leadership. Seminar participants will be able to indicate session preference during the check-in process. Please see descriptions below for intended audiences.

Security/Compliance | Intended for university research compliance, research administration, facility security, research security, and export control professionals.

Cyber Security | Intended for information security officers, computer incident response teams, information system security managers

Executive Leadership | Intended for Vice Presidents for Research and Provosts.
Scientific discovery and innovation are based on open and reciprocal exchange of information and ideas...except when they aren’t. Foreign talent recruitment programs, intellectual property theft, trade wars, economic sanctions, election hacking - all threaten the principles of openness and transparency that academic research communities are built upon. How do we communicate effectively with faculty members about the stuff we are all seeing in the news?

The openness of the US academic community also makes it a target for influence and interference by some foreign governments. Some foreign governments have attempted to influence and interfere on campuses in ways which can directly infringe on the rights of students, limit free speech, and affect the content of faculty teaching and affect academic activities and content. This panel will discuss issues to consider in ensuring your university and departments are limiting foreign influence and safeguarding academic freedom on campus.

As part of its ongoing effort to keep international research collaboration both open and secure, the National Science Foundation (NSF) commissioned a report by the independent science advisory group JASON to enhance the agency’s understanding of the threats to basic research posed by foreign governments that have taken actions that violate the principles of scientific ethics and research integrity. This featured presentation will cover findings and recommendations of this study.

This presentation will provide an overview of vectors of technology and know-how transfers that largely fall outside U.S. intelligence, counterintelligence, law enforcement, export control, or other regulatory oversight. Examples of state-directed influence and penetration of (primarily) federally funded research in academia will be provided, as well as research collaboration that undermines academic integrity and ethics and threatens U.S. national security. A key challenge facing U.S. research institutions is that the highlighted examples are most likely legal, though some may violate administrative or grant compliance provisions.

U.S.-based scholars are co-authoring science and technology research with counterparts at seven PRC universities that are intimately tied to the PRC’s defense industrial base and weapons development programs. Prevailing risk management and due diligence frameworks are inadequate to these circumstances because, while these collaborations may be reckless on national security grounds, most are nevertheless lawful. What does this grey zone look like, and how should we navigate it?

This presentation will discuss Lockheed Martin’s award-winning Counterintelligence program, focusing on the establishment, governance, and program execution. It will also cover efforts to partner with the academic community; tapping into their diverse and collaborative environments to further the company’s research and development objectives, while ensuring sensitive information is properly safeguarded.

The U.S. bioeconomy increasingly serves as a critical foundation for American competitiveness, security, economic growth, and global leadership in research and innovation. The bioeconomy—spanning health care, information systems, agriculture, manufacturing, national defense, and beyond—is growing rapidly with increasing impact on our country’s prosperity and health. However, along with the amazing promise, there are associated security challenges, many of which have not been identified or fully defined. The FBI will provide broader awareness of the bioeconomy security issue and highlight the importance of building partnerships between the academic, private sector, and law enforcement communities.

Modern systems are very challenging to protect and defend. Serving as a security engineer requires understanding core principles and applying them in creative ways. This talk will present some principles, illustrating them with example of application to a Smart City infrastructure, followed by informed discussion.

Registration is available on the ASCE Web site: https://asce.tamu.edu/conference/