CSET CENTER for SECURITY and EMERGING TECHNOLOGY

SUBJECT: Establishing a new public-private institution to improve American research security
FROM: Melissa Flagg and Zachary Arnold

BACKGROUND

- U.S. adversaries are extracting valuable data, know-how, and intellectual property from American research institutions, including businesses, universities, and government labs.
- Currently, federal authorities address this issue by prosecuting researchers who conceal relationships with Chinese entities, investigating research institutions, restricting visas for certain Chinese students and researchers, and conducting outreach to university administrators.

KEY POINTS

- ***Federal authorities can't secure American research on their own.***
  - Federal agencies and law enforcers have limited and uneven authority over most U.S. R&D: federal jurisdiction typically relies on the presence of federal research funding, but federal funding has limited reach, especially in the large industrial R&D space.
    - 90% of R&D occurs outside of government, mainly in industry (73%) and universities (13%).
    - The federal government funds 51% of university R&D, but only 22% of total U.S. R&D.
  - FBI Director Wray emphasizes the need for "a whole-of-society response [to research security threats], with government and the private sector working together."
- ***Many, if not most, researchers will not proactively collaborate with law enforcement.***
  - A 2009 survey by the Federation of American Scientists and the FBI concluded that "scientists are suspicious of the FBI and feel that they do not work well with the scientific community."
  - Law enforcement often lacks the expertise to assess suspicious activity within R&D. In the 2009 survey, 76% of respondents agreed that law enforcement "[did] not understand their work."
- ***Researchers need support that is difficult for law enforcement and intelligence agencies to provide.***
  - Federal authorities have limited or no jurisdiction over Chinese technology transfer strategies, which are often legal (or at least not clearly *illegal*).
  - Classification and confidentiality concerns frequently prevent federal agencies from sharing actionable "threat intelligence" with researchers and their institutions.

RECOMMENDATIONS

- ***Convene and fund an independent, public-private institution to inform and support research security efforts throughout America's R&D ecosystem.***
  - The institution should:
    - Provide researchers and their institutions with context-specific, data-driven threat assessments, allowing them to assess risks to research security in any specific situation.
    - Track security trends and threats across the U.S. research landscape, whether or not those threats implicate violations of law, and develop and disseminate defensive best practices.
    - Employ staff with technical expertise and experience in R&D, counterintelligence, data visualization, and open-source data analysis.
  - Potential models include but are not limited to public-private cybersecurity operations centers, industry self-regulatory bodies, and intelligence "fusion centers."
  - To win the research community's trust and ensure the greatest possible scope of action, the institution must be meaningfully independent from law enforcement.
- ***As an initial step, survey the research community to identify the most important unmet needs and opportunities in research security.***