KILPATRICK TOWNSEND

4 KEY TAKEAWAYS

U.S. Government Enforcement Related to Research

Kilpatrick Townsend partners Adria Perez and Clay Wheeler recently presented "Criminal Enforcement Trends in a Connected World" at the firm's Kilpatrick Townsend Intellectural Property Seminar (KTIPS). KTIPS is an intensive, two-day patent strategy and protection seminar designed to provide insightful and in-depth training related to current developments in patent law, and how those impact patent procurement and enforcement strategies.

Ms. Perez and Mr. Wheeler presented on numerous topics specifically related to criminal enforcement laws and trends. Below are key takeaways from one of the more compelling issues discussed, **"U.S. Government Enforcement Related to Research Integrity and Security:"**

1

Foreign influence is still a DOJ priority despite the name change. "Foreign influence" can occur when a foreign government inappropriately influences or undermines U.S. democratic, economic, and scientific institutions, including U.S. federally-funded research. Earlier this year, the DOJ announced that the "China Initiative," the enforcement initiative to counter the theft of U.S. government-funded technologies by the Chinese government, has been renamed as the "Strategy for Countering Nation-State Threats." The strategy focuses not only on China, but also Russia, North Korea, and Iran. Despite the name change, combating foreign nation state influence is still a priority to the DOJ.

2

Research integrity and security is a national security issue. Since national security issues tend to have bi-partisan support, Congress is able to allocate more funds and resources to the DOJ, including more agents and attorneys, to focus on enforcement. The DOJ's National Security Division has an active supervisory role in research integrity and security matters, and works closely with the FBI and other investigative agencies to determine whether the case should be a civil or administrative matter or if criminal prosecution is warranted. This additional oversight may cause some investigations to proceed more slowly.

3

Examples of research integrity and security issues that can lead to enforcement efforts against institutions, companies and individuals. The following is a non-exclusive list of research integrity and security issues that will get the attention of U.S. law enforcement:

- False statements in federal grant applications by:
  - ◊ Concealing foreign government-affiliated university employment and foreign research grants; and
  - ◊ Hiding foreign government program participation, such as in China's Thousand Talents Program.
- False statements made to U.S. authorities, such as the FBI, concerning:
  - ◊ Patents filed overseas using a scientist's birth name; and
  - ◊ Participation in foreign government programs, such as China's Thousand Talents Program;
- Undisclosed conflicts of interest, including undisclosed positions and equity interests in foreign companies that should have been subject to a conflict-of-interest disclosure;
- Violations of peer-review-integrity rules, such as sending confidential information abroad after signing a certification that the data would not be shared;
- Providing falsified research results to U.S. government agencies to procure federal dollars;
- Failing to comply with the federal government's cybersecurity requirements despite certifications;
- Failing to file reports of foreign bank and financial accounts with the IRS;
- Submitting false income tax returns by not reporting foreign income; and
- Taking research-related electronic files overseas.

The DOJ may use the theft of trade secrets and economic espionage statutes, the False Claims Act, or common law approaches, such as breach contract or fraud in the inducement, to combat these issues.

4

How to protect your institution and company. Institutions and companies need to implement reasonable compliance efforts to identify and prevent research integrity and security issues, including:

- Thorough review of grant proposals and awards, including instituting controls to ensure compliance with the grant requirements;
- Thorough conflict-of-interest disclosure procedures;
- Mandatory training for principal investigators, researchers and engineers to ensure they understand the consequences of any research integrity and security issues;
- Data analytics that tracks and raises any anomalies concerning grant awards, travel, expenses and leaves of absences for principle investigators, researchers and engineers;
- Effective whistleblower and investigative programs; and
- Cybersecurity controls that meet federal government requirements.

For more information, please contact:
Adria Perez: aperez@kilpatricktownsend.com.
Clay Wheeler: cwheeler@kilpatricktownsend.com