Statement for the Record

Brenna E. Jenny, Deputy Assistant Attorney General, Civil Division, U.S. Department of Justice

Before U.S. House of Representatives Science, Space, and Technology Hearing

June 24, 2026

Thank you for the invitation to testify at today's hearing about the steps the U.S. Department of Justice (Department), Civil Division is taking to combat fraud involving federal research grants.

I serve as the Deputy Assistant Attorney General for the Commercial Litigation Branch of the Civil Division. In that role, I supervise the Civil Fraud Section, which leads the Department's enforcement of the federal False Claims Act (FCA). The FCA is a flexible enforcement tool that allows us to redress a range of fraud and abuse in federal government programs, contracts, grants, and loans. The FCA provides for liability based on knowingly submitting a false claim and allows the government to collect three times the amount of its damages, plus civil statutory penalties. The concept of a "claim" under the FCA has been broadly construed by courts. Relevant to the context of federal research grants, an application to receive a grant or a request to draw down funds could all be considered a claim. Those claims can be rendered false if the grant recipient violates some applicable legal obligation. For example, if a grantee expressly certifies in a grant application that it will comply with certain rules, and it fails to do so, that can create FCA liability. But FCA liability is not limited to situations where a grantee makes an affirmative false statement. If a grantee omits material information, that can also cause a claim to be false.

To establish liability, the government must also show that the violation of a statutory, regulatory, or contractual requirement was material to the government's payment decision. In other words, that the violation has a natural tendency to influence, or be capable of influencing, the government's payment to the grantee. Finally, the grantee must act with the requisite scienter, which requires proof of at least reckless disregard. Negligence is insufficient.

Single damages are typically the difference between the amount the government paid and the amount it would have paid had it known the truth about the grantee's noncompliance. Courts also look at how much value the government received notwithstanding the falsity/non-compliance with the requirement. There may be questions about the measure of the government's damages in these cases, particularly where the government received the research that it paid for, notwithstanding a recipient's failure to comply with certain disclosure requirements. But even if damages cannot be precisely quantified, that does not mean the government did not suffer harm from the violations. The FCA is the government's primary civil tool to recover losses due to fraud and abuse by persons seeking payment from the United States. In Fiscal Year 2025, across all FCA settlements and judgments, the United States achieved a record recovery of more than $6.8 billion.

FCA matters generally originate from one of three primary sources. First, the FCA contains a qui tam provision that allows private persons to file sealed complaints in federal district court and for the government to investigate and decide whether to take over the cases. Whistleblowers may be awarded 15 to 30 percent of the government's recovery. Historically, most whistleblowers were insiders who personally witnessed fraud and came forward to file a complaint. Recently, data miners are increasingly serving as whistleblowers, and by that I mean, individuals who analyze public data and information and file qui tam complaints. Both types of whistleblowers play an important role in our pipeline of incoming cases.

The second primary source of new FCA cases are agency referrals. Agencies have robust programs to identify and manage potential false claims. They have Offices of Inspectors General (OIGs), whose mission is to protect the integrity of the programs being administered. Within OIG or in addition to it, most agencies also have an office responsible for auditing ongoing contracts and grants. These offices are staffed by highly skilled agents and auditors with years of experience overseeing particular government programs. When OIGs or audit offices detect potential anomalies or receive tips about fraud, they will investigate them and make referrals to the Department. Finally, the Department initiates some FCA investigations based on information sources such as data analytics or by developing leads through other investigations into parties engaging in similar fraud schemes.

Fraud involving federal research grants can implicate a diverse range of misconduct. Some areas that have been a focus for the Department recently include failure to disclose foreign funding, falsifying research data and images, and violations of cybersecurity requirements.

Failure to Disclose Foreign Funding: Section 117 of the Higher Education Act of 1965 requires that any research institution receiving federal funding must disclose all contracts or gifts from foreign sources that exceed $250,000 (singly or combined from one source) in a calendar year. In addition, applicants for grants from federal agencies typically must disclose "all current and pending support," and the disclosure obligation is not limited to support for work the grantee seeks to be funded by a federal grant. This requirement applies broadly to grants agencies award, including the National Aeronautics and Space Administration (NASA), the National Institutes of Health (NIH), and the National Science Foundation (NSF). In addition, a recipient of NASA funds must certify that it will not "participate, collaborate, or coordinate bilaterally in any way with China or any Chinese-owned company." This is a result of Section 1340 of the Department of Defense and Full-Year Continuing Appropriations Act, 2011 (Public Law 112-10).[1] Grantees certify they are complying with these requirements, as applicable, and knowing non-compliance may form the basis for FCA liability, provided the agency confirms that compliance was material for the specific grant under investigation.

[1] Note, this was most recently extended in Section 526 of the Commerce, Justice, Science; Energy and Water Development; and Interior and Environment Appropriations Act, 2026 (Public Law 119-74).

An example of a resolved case in this space is a $7.6 million settlement the Department entered into in 2024 with a hospital resolving allegations that the hospital failed to disclose to NIH in grant applications and Research Performance Progress Reports that the Principal Investigator had current and pending support from foreign sources. The Civil Fraud Section continues to investigate both whistleblower allegations and referrals from our agency clients in this area.

Falsifying Research Data/Images: Grantees have an obligation to accurately describe data and prior related research when applying for new grant funding. Doing so is important because it allows granting agencies to fairly compare grant applications and make decisions about which research is the most promising and deserving of funding. The Civil Division has multiple active investigations reviewing allegations of falsified or manipulated images that were used in grant applications.

For example, a cancer research and treatment center paid $15 million to resolve allegations that the center used funds from six NIH grants to conduct research that resulted in 14 publications in scientific journals containing misrepresented and/or duplicated images and data. The center also admitted that one of its researchers received four NIH grants after submitting grant applications that discussed a journal article containing misrepresentations.

Violations of Government Cybersecurity Requirements: While not limited to government grants, this is an area where the Department has seen significant growth in the last several years. The Department announced the Civil Cyber-Fraud Initiative in 2021. The goal of the initiative is to leverage the FCA to penalize grantees and contractors that fail to comply with cybersecurity requirements. When a government grant or contract involves the use of sensitive government data or personal health information, it is common for that grant or contract to impose specific cybersecurity requirements on the recipient of the federal funds. Grantees and contractors that knowingly submitted a claim to the government despite not satisfying cybersecurity obligations can be liable under the FCA. The FCA is an important tool for the government in this context because a grantee's violation of cybersecurity requirements potentially jeopardizes the security of government data or information systems, and the government does not receive the level of security it bargained for under the grant.

Over the past five years, the Department has settled 15 cyber fraud matters, for total settlements of over $73.5 million. In addition, one qui tam relator settled a cyber fraud case during that period for $9 million. Of those matters, two cyber fraud cases related to universities or other research institutions; those matters were settled for over $2 million. During this period, the Department also opened numerous, non-public, cyber fraud matters.

***

The Department is committed to protecting the integrity of federally funded research and ensuring that taxpayer dollars are used for their intended purposes. The Department will continue to work with law enforcement partners, agency Inspectors General, and whistleblowers to identify fraud by grant recipients and safeguard the public's investment in scientific innovation and discovery.