



SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HEARING CHARTER

“Safeguarding Federal Research Funds: The False Claims Act's Role in Combating Grant Fraud”

June 24, 2026

10:00 a.m.

2318 Rayburn House Office Building

Purpose

This hearing will examine federal law enforcement agencies' use of the False Claims Act (FCA) to combat fraud and misconduct involving federally funded research. The hearing will explore grant fraud involving false certifications and material misrepresentations in applications for federal research funding; failures by institutions to disclose foreign gifts, contracts, and sources of support as required by federal law; and cybersecurity noncompliance by universities, contractors, and other research performers receiving federal funds. The hearing will also review recent FCA enforcement actions involving research institutions, assess the effectiveness of current oversight and enforcement mechanisms, and consider potential legislative and administrative reforms to strengthen accountability, improve transparency, protect research integrity and national security, and safeguard taxpayer-funded research programs.

Witnesses

- **Robert Steinau**, Senior Official Performing the Duties of Inspector General, National Aeronautics and Space Administration Office of the Inspector General
- **Jennifer Springmann**, Special Agent in Charge, National Science Foundation Office of the Inspector General
- **Brenna Jenny**, Deputy Assistant Attorney General for Commercial Litigation Branch, Department of Justice

Overarching Questions

- How does fraud and misconduct affect federally funded research programs, and are current mechanisms sufficient to detect, deter, and address grant fraud, false certifications, and other material misrepresentations?

- How effective is the Department of Justice's use of the False Claims Act to hold research institutions, contractors, and grant recipients accountable for violations of federal requirements, and are additional enforcement tools or authorities needed to strengthen accountability?
- Are universities and other recipients of federal research funding adequately disclosing foreign sources of support, affiliations, and financial relationships as required by federal law, and what risks do disclosure failures pose to research integrity, taxpayer interests, and national security?
- Are federally funded research institutions meeting their obligations to protect sensitive data, intellectual property, and government information, and does current False Claims Act enforcement provide sufficient incentives to ensure compliance with cybersecurity and research security requirements?

Background: An Overview of the False Claims Act

The False Claims Act (FCA), 31 U.S.C. §§ 3729–3733, was originally enacted in 1863 to combat supplier fraud against the Union Army during the Civil War.¹ It has since evolved into the federal government's primary tool for policing fraud against government programs, including federally funded research. The FCA imposes liability on any person who knowingly submits, or causes the submission of, false or fraudulent claims for payment to the government.² Violations carry steep penalties, currently ranging from \$13,946 to \$27,894 per false claim.³

A cornerstone of the FCA is its *qui tam* provision, which allows private citizens, known as relators or whistleblowers, to file suit on behalf of the government and share in any resulting recovery.⁴ *Qui tam* suits are instrumental in uncovering research fraud that government auditors might otherwise not detect.⁵ In 2025, the Department of Justice (DOJ) announced a record \$6.8 billion in FCA settlements and judgments, marking the highest single-year total recovery of federal funds since the law's enactment.⁶

The scale of federal fraud exposure is significant. A 2024 GAO report (GAO-24-105833) estimated that the federal government loses between \$233 billion and \$521 billion annually to

¹ U.S. Dep't of Just., The False Claims Act: A Primer, https://www.justice.gov/d9/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf.

² *Id.*

³ *Id.*

⁴ Fed. Law Enf't Training Ctrs., An Overview of “Qui Tam” Actions, https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/civil-actions/quitam.pdf.

⁵ Benjamin McCoy et al., *Blowing the Whistle: A Primer on the False Claims Act*, THE TEMPLE 10-Q (2019) <https://law.temple.edu/10q/blowing-the-whistle-a-primer-on-the-false-claims-act/>.

⁶ Press Release, U.S. Dep't of Just., False Claims Act Settlements and Judgements Exceed \$6.8B in Fiscal Year 2025 (Jan. 16, 2026), <https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-68b-fiscal-year-2025>.

fraud based on 2018–2022 data across various risk environments.⁷ Research grant programs administered by the Department of Defense (DOD), National Aeronautics and Space Administration (NASA), National Science Foundation, Environmental Protection Agency (EPA), and the Department of Energy represent a meaningful subset of that exposure. The FCA's broad applicability to grant and contract recipients, including universities, makes it a particularly potent tool for addressing fraudulent misconduct in the research ecosystem.

Legal experts identify three broad compliance risk areas under the FCA relevant to research institutions: false certifications regarding eligibility, performance, or regulatory compliance; fraudulent billing or mischarging of costs to federal grants; and the failure to disclose material information required by the terms of a grant award.⁸ Each of these risk categories frequently serves as the basis for FCA enforcement actions.

Grant Fraud and False Certifications

Grant fraud under the FCA most commonly involves false certifications, which are false representations made in grant applications or progress reports submitted as a condition of receiving federal funds.⁹ When an institution knowingly misrepresents facts material to the government's decision to award a grant, it may face FCA liability even if the underlying research is legitimate.¹⁰ For example, a recent FCA settlement involving the Dana-Farber Cancer Institute highlighted that misstatements or omissions in federal grant applications, particularly regarding required disclosures and compliance certifications, can create FCA liability even in the absence of intent to defraud.¹¹ The case illustrates that weaknesses in institutional oversight and internal controls over grant submissions can be sufficient to trigger liability when false or misleading representations are made to secure federal funding.

The Duke University case remains one of the most consequential FCA settlements in the research context. In 2019, the DOJ announced that Duke agreed to pay \$112.5 million to settle allegations that it submitted falsified research data and manipulated grant applications to the National Institutes of Health (NIH), EPA, and DOD over a period of years.¹² The case originated from a

⁷ *FRAUD RISK MANAGEMENT: 2018-2022 Data Show Federal Government Loses an Estimated \$233 Billion to \$521 Billion Annually to Fraud, Based on Various Risk Environments*, GAO-24-105833, U.S. GOV'T. ACCOUNTABILITY OFF. (April 2024), [GAO-24-105833, FRAUD RISK MANAGEMENT: 2018-2022 Data Show Federal Government Loses an Estimated \\$233 Billion to \\$521 Billion Annually to Fraud, Based on Various Risk Environments](https://www.gao.gov/products/GAO-24-105833).

⁸ Preston Pugh et al., *The False Claims Act: compliance issues in US government procurement and healthcare*, Global Investigations Review (Sept. 9, 2025), [Global Investigations Review](https://www.gir.com/en/articles/view/the-false-claims-act-compliance-issues-in-us-government-procurement-and-healthcare).

⁹ See Nadia Patel et al., *What Nonprofits Receiving Federal Funds Need to Know About the False Claims Act*, Arent Fox Schiff (Mar. 26, 2026), <https://www.afslaw.com/perspectives/alerts/what-nonprofits-receiving-federal-funds-need-know-about-the-false-claims-act>.

¹⁰ *Id.*

¹¹ Press Release, U.S. Dep't of Just., Dana-Farber Cancer Institute Agrees to Pay \$15M to Settle Fraud Allegations Related to Scientific Research Grants (Dec. 16, 2025), <https://www.justice.gov/opa/pr/dana-farber-cancer-institute-agrees-pay-15m-settle-fraud-allegations-related-scientific>.

¹² Press Release, U.S. Dep't of Just., Duke University Agrees to Pay U.S. \$112.5 Million to Settle False Claims Act Allegations Related to Scientific Research Misconduct (Mar. 25, 2019),

qui tam relator and former Duke employee and illustrates both the power of whistleblowers and the severity of consequences for research misconduct.¹³

Foreign Funding Nondisclosure

Section 117 of the Higher Education Act requires institutions of higher education receiving federal financial assistance to disclose gifts and contracts from foreign sources totaling \$250,000 or more from a single source in a calendar year.¹⁴ DOJ has pursued multiple enforcement actions against institutions that concealed foreign funding while receiving federal research grants, raising serious concerns about foreign influence in U.S. research programs.¹⁵

A few notable cases demonstrate the scope of the issue. In October 2023, Stanford University agreed to pay \$1.9 million to resolve allegations that it failed to disclose current and pending foreign research support received by twelve faculty members in federal grant proposals.¹⁶ In May 2024, Cleveland Clinic agreed to pay over \$7 million to settle allegations that researchers failed to disclose foreign funding sources — including from Chinese entities — on NIH grant applications and reports.¹⁷ Similarly, in 2024, DOJ alleged that three University of Maryland researchers failed to disclose that their federally funded projects were also receiving support from foreign companies.¹⁸

The scope of undisclosed foreign funding at American universities is substantial. The Department of Education’s most recent foreign funding disclosure release documented more than \$5.2 billion in foreign funding reported by U.S. colleges and universities for 2025 alone.¹⁹ These figures represent only disclosed amounts; enforcement cases suggest significant non-compliance persists.²⁰ A 2020 GAO report (GAO-21-130) found that federal research agencies had

<https://www.justice.gov/archives/opa/pr/duke-university-agrees-pay-us-1125-million-settle-false-claims-act-allegations-related>.

¹³ *Id.*

¹⁴ Section 117 of the Higher Education Act, 20 U.S.C. § 1011f (2026).

¹⁵ See Marcus Funk et al., *Universities in the crosshairs: Navigating foreign espionage and research security risks*, The Compliance and Ethics Blog (Jun. 3 2026), <https://complianceandethics.org/universities-in-the-crosshairs-navigating-foreign-espionage-and-research-security-risks/>.

¹⁶ Press Release, U.S. Dep’t of Just., Stanford University Agrees to Pay \$1.9 Million to Resolve Allegations That it Failed to Disclose Foreign Research Support in Federal Grant Proposals (Oct. 2, 2023), <https://www.justice.gov/archives/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign>.

¹⁷ Press Release, U.S. Dep’t of Just., Cleveland Clinic to Pay Over \$7 Million to Settle Allegations of Undisclosed Foreign Sources of Funding on NIH Grant Applications and Reports (May. 17 2024), <https://www.justice.gov/usao-ndoh/pr/cleveland-clinic-pay-over-7-million-settle-allegations-undisclosed-foreign-sources>.

¹⁸ Press Release, U.S. Dep’t of Just., University of Maryland, College Park Agrees to pay \$500,000 to Resolve Allegations That It Failed to Disclose Foreign Research Support in Federal Grant Proposals (Jul. 16, 2024), <https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed>.

¹⁹ Press Release, U.S. Dep’t of Ed., U.S. Department of Education Releases Latest Foreign Funding Disclosures from Federally-Funded American Universities (Feb. 11, 2026), <https://www.ed.gov/about/news/press-release/us-department-of-education-releases-latest-foreign-funding-disclosures-federally-funded-american-universities>.

²⁰ See *Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence* GAO-21-130, U.S. GOV’T. ACCOUNTABILITY OFF. (Dec. 17, 2020), <https://www.gao.gov/products/gao-21-130>.

inadequate policies to address foreign influence, and recommended improvements to disclosure and oversight frameworks.²¹ A subsequent 2024 GAO report (GAO-24-106227) found that strengthened interagency collaboration is needed to safeguard federal research funding from foreign threats, noting persistent gaps in coordination among the agencies responsible for research security.²² The core policy concern is not international collaboration itself, but whether federal agencies have complete and accurate information when evaluating grant applications and overseeing award performance. Undisclosed foreign affiliations or funding sources may affect agency assessments of conflicts of interest, intellectual property risks, and potential foreign government influence.

Cybersecurity Noncompliance

Federal agencies increasingly require contractors and grant recipients handling sensitive research data to comply with specific cybersecurity frameworks, particularly the National Institute of Standards and Technology (NIST) SP 800-171 standard for Controlled Unclassified Information (CUI).²³ False certifications of compliance with these requirements may constitute FCA violations, particularly when an institution knowingly misrepresents its cybersecurity posture to obtain or retain federal contracts or grants.²⁴

In October 2024, Pennsylvania State University agreed to pay \$1.25 million to resolve FCA allegations that it failed to comply with cybersecurity requirements in fifteen contracts and subcontracts involving DOD and NASA.²⁵ In October 2021, DOJ launched the Civil Cyber-Fraud Initiative specifically to hold accountable contractors and grantees who misrepresent or fail to meet cybersecurity standards, putting sensitive government information and national security at risk through FCA enforcement mechanisms.²⁶ The initiative reflects DOJ's recognition that cybersecurity noncompliance by research institutions poses systemic risks beyond a particular grant or contract.²⁷

²¹ *Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence* GAO-21-130, U.S. GOV'T. ACCOUNTABILITY OFF. (Dec. 17, 2020), <https://www.gao.gov/products/gao-21-130>.

²² *Research Security: Strengthening Interagency Collaboration Could Help Agencies Safeguard Federal Funding from Foreign Threats*, GAO-24-106227, U.S. GOV'T. ACCOUNTABILITY OFF. (Jan. 11, 2024), <https://www.gao.gov/products/gao-24-106227>.

²³ Nat'l Inst. of Standards and Tech, NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (2024).

²⁴ See Eoin P. Beirne et al., "False" Sense of Security: DOJ Announces False Claims Act Settlement Related to Failure to Comply with Cybersecurity Requirements, Mintz (Aug. 4, 2025), <https://www.mintz.com/insights-center/viewpoints/2146/2025-08-04-false-sense-security-doj-announces-false-claims-act>.

²⁵ Press Release, U.S. Dep't of Just., The Pennsylvania State University Agrees to Pay \$1.25M to Resolve False Claims Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements (Oct. 22, 2024), <https://www.justice.gov/archives/opa/pr/pennsylvania-state-university-agrees-pay-125m-resolve-false-claims-act-allegations-relating>.

²⁶ See Press Release, U.S. Dep't of Just., Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), <https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>.

²⁷ See Shawna Chen, *DOJ launches new initiative to target contractor cyber-fraud*, Axios (Oct. 6, 2021), <https://www.axios.com/2021/10/06/doj-cyber-fraud-government-contractor>.

Moreover, DOJ's Civil Rights Fraud Initiative, established in May 2025, expanded the application of the FCA to institutions that certify compliance with federal civil rights requirements as a condition of receiving federal funding, including universities and research institutions.²⁸ This initiative reflects the FCA's continued evolution as an enforcement tool beyond traditional financial fraud.

Legislative and Oversight Context

The growing number of FCA cases involving universities, research institutions, and federal grant recipients illustrates the expanding intersection between research compliance, research security, and fraud enforcement. Traditionally associated with procurement fraud and healthcare fraud, the FCA is increasingly being used to address a broader range of conduct in the research context, including falsified data, undisclosed foreign funding and affiliations, cybersecurity deficiencies, and other material misrepresentations made in connection with federal awards. These cases show that federal agencies rely heavily on the accuracy of information provided by applicants and recipients when making funding decisions, monitoring grant performance, and protecting sensitive government-funded research and related information.

As federal investments in scientific research continue to increase, questions remain regarding the adequacy of existing disclosure requirements, compliance systems, and oversight mechanisms. Disclosure obligations differ across funding agencies, creating inconsistencies that can complicate both institutional compliance efforts and federal enforcement. Meanwhile, the research landscape has grown increasingly complex, presenting challenges that existing frameworks may not fully address. Policymakers, federal agencies, and research institutions continue to debate how best to balance scientific collaboration and innovation with transparency, accountability, research integrity, and national security. The hearing will examine whether current laws, regulations, and oversight mechanisms are sufficient to meet these challenges and protect taxpayer-funded research.

²⁸ Press Release, U.S. Dep't of Just., Justice Department Establishes Civil Rights Fraud Initiative (May. 19, 2025), <https://www.justice.gov/opa/pr/justice-department-establishes-civil-rights-fraud-initiative>.