NASA

National Aeronautics and Space Administration

Office of Inspector General

**Testimony before the House of Representatives
Subcommittee on Investigations and Oversight,
Committee on Science, Space, and Technology**

SAFEGUARDING FEDERAL RESEARCH FUNDS: THE FALSE CLAIMS ACT'S ROLE IN COMBATING GRANT FRAUD

Statement of Robert H. Steinau

Senior Official Performing the Duties of Inspector General

National Aeronautics and Space Administration

**For Release on Delivery (expected at 10 a.m.)
June 24, 2026**

Chairman McCormick, Ranking Member Sykes, and Members of the Subcommittee:

As NASA's independent oversight authority, the Office of Inspector General (OIG) safeguards the Agency's research funds, combats grant fraud, and ensures federal resources are awarded fairly and responsibly. This charge is more important than ever following the success of Artemis II. As NASA propels Americans to the Moon and beyond, the OIG protects taxpayer-funded research here on Earth from fraudsters and foreign adversaries threatening national security. I welcome the opportunity to share our vital work in this area, and I am grateful to the hardworking OIG employees who ensure NASA's scientific partners follow federal requirements to secure sensitive government information.

While America's open research environment drives innovation and establishes the nation's dominance as a global leader, the government must enforce strict oversight boundaries to maintain this competitive edge. In 2011 Congress passed a law, colloquially known as the Wolf Amendment, which prohibits NASA from using federal funds to engage in bilateral research, cooperation, or coordination with Chinese entities unless authorized by Congress and the Federal Bureau of Investigation.[1] The prohibition applies to a wide range of activities involving China, including joint research, data sharing, personnel exchanges, training, and conferences. Together with other federal requirements, this means institutions may be ineligible for awards if they submit research proposals involving cooperation with China or fail to disclose foreign affiliations.

Each year, NASA awards thousands of research grants and cooperative agreements that fuel innovation at institutions across the country. In fiscal year 2025 alone, the Agency furnished over 1,700 new awards and obligated over $1.3 billion. Over the last decade, the Agency's total assistance obligations have exceeded $10 billion.

The breadth and scale of these research awards underscore the significant challenge NASA faces in protecting its resources and intellectual property from foreign influence. As beneficiaries of federal funds, institutions and contractors are responsible for maintaining transparency and accountability by disclosing foreign sources of support, affiliations, and financial relationships. To ensure applicants for grants and cooperative agreements understand the Wolf Amendment, the Agency provides clear, publicly accessible guidance online and in its Grant and Cooperative Agreement Manual.[2]

In addition, NASA funding is conditioned on restrictions that contractors and grant recipients are not affiliated with China or a Chinese-owned company, and that they will not participate, collaborate, or coordinate bilaterally with China or any Chinese-owned company. By submitting their business proposals, the contractors and grantees represent that they are in compliance with these restrictions. When award recipients misrepresent themselves or their work, they jeopardize both NASA's scientific integrity and America's preeminence in space.

[1] Department of Defense and Full-Year Continuing Appropriations Act, 2011, Pub. L. No. 112-10, § 1340 (2011).

[2] NASA, *NASA Grant and Cooperative Agreement Manual* (GCAM) (March 21, 2025).

Because NASA relies on its research partners to report possible conflicts of interest, the OIG is a critical fail-safe to identify those who do not submit complete and truthful grant and contract applications. Although today's testimony focuses on threats to research security, the OIG pursues many types of grant fraud allegations, which have included specific offenses of false claims, false statements, wire fraud, mail fraud, and export control violations, as well as uncovering contractor misconduct and general security violations.

Over the last decade, the OIG has opened more than 120 grant fraud cases totaling over $14 million in monetary impact, with nearly $5 million recovered for NASA. This is just a small subset of the vast portfolio of fraud cases the OIG has investigated in this time. During that same period, we also issued four audits examining cooperative agreements. Together, these reports reviewed nearly $1 billion of NASA funds to research institutions, resulting in over $16 million in questioned costs and 24 recommendations aimed at strengthening financial, governance, performance monitoring, and personnel controls.

After identifying research security gaps, the OIG leverages a broad suite of tools to hold institutions, contractors, and grant recipients accountable. In some cases, our investigators will coordinate with NASA management to seek administrative remedies, corrective actions, and policy changes. In other cases, the OIG will refer its findings to the Department of Justice (DOJ) for prosecution, which can result in criminal indictments, prison time, steep fines, and additional penalties. Violators can be subject to both criminal and civil penalties for the same offenses. They may also be administratively suspended or permanently debarred from receiving future federal grants and contracts.

In lieu of criminal prosecution, the OIG and DOJ may opt to pursue civil lawsuits under the False Claims Act (FCA) when a person knowingly submits, or causes to submit, false claims to the government.[3] This allows the government to recover up to three times the damages, in addition to a penalty linked to inflation.

The FCA's broad scope makes it an effective tool to counter grant and contract fraud. For example, it can be used to penalize those who misrepresent themselves on grant applications, falsify costs (e.g., overcharging) and progress reports, fabricate data (e.g., test results), substitute inferior or defective parts, or compromise NASA's cybersecurity. In the last decade, the OIG recovered over $22 million in civil settlements, the majority of which were pursued under the FCA.

The FCA also includes a *qui tam* provision, which allows whistleblowers, such as contractors or research institution affiliates, to file a lawsuit on behalf of the government and provides them with protection from retaliation. The OIG investigates these whistleblower tips. If the government recovers funds, the whistleblower is generally entitled to a portion of the amount based on the degree to which the prosecution's success is based on the tip. Over the last 15 years, the OIG experienced a seven-fold increase in monetary results from *qui tam* actions, averaging $7.4 million in resolutions per year. Over the last 5 years alone, we opened nearly 50 *qui tam* investigations.

My testimony today focuses on the OIG's top three research oversight priorities, which are essential to closing critical security gaps and preserving scientific integrity across NASA-funded programs.

[3] DOJ, *The False Claims Act* (accessed June 18, 2026) https://www.justice.gov/civil/false-claims-act.

Combating Rising Fraud Through Enhanced Deterrence Initiatives

Targeting fraud and misconduct in NASA-funded research projects has been a core mission for the OIG since its establishment nearly half a century ago. Today, one of our top priorities continues to be implementing initiatives that enhance fraud identification and deterrence. As the threat landscape has evolved, so too have our detection strategies, allowing us to uncover and proactively pinpoint a growing number of research security issues.

Since 2018, our research security caseload has increased seven-fold. During this time, we initiated nearly 100 investigations in this area related to foreign influence, resulting in a monetary impact of over $11 million with nearly $2 million recovered for the Agency. Our investigations frequently reveal that universities and principal investigators make false certifications or omit required disclosures, intentionally or unintentionally misrepresenting compliance with statutory restrictions.

In one recent case, the University of Delaware agreed to pay $715,580 to resolve allegations under the FCA that it did not disclose a professor's ties to China.[4] Over the course of a decade, the university had applied for multiple NASA grants and engaged in cooperative agreements listing the professor as a co-principal investigator. The OIG's investigation revealed that the professor was also a faculty member at a Chinese university and was receiving funding from the Chinese government. Moreover, he was participating in the Thousand Talents Program—a Chinese initiative that recruits individuals with knowledge of or access to foreign technology. As a result of the case, NASA received over $300,000 of restitution and the OIG halted further spread of scientific information to foreign entities.

To bolster grant and contract fraud detection, the House Select Committee on China has called for a joint OIG-DOJ task force to investigate potential research security risks.[5] We welcome this opportunity for interagency collaboration, as it is a powerful force multiplier to advance complex, high-stakes investigations. We look forward to working closely with the DOJ to continue protecting NASA's valuable resources.

In addition, the OIG is reviewing the feasibility of initiating a new body of work dedicated to proactive grant, contract, and cooperative agreement oversight. This initiative would likely entail conducting site visits to institutions and awardees receiving NASA funding. This would allow us to verify that award recipients are complying with federal and Agency requirements, including cybersecurity mandates and foreign disclosure rules. If violations are identified, our investigators and law enforcement partners would work together to hold wrongdoers accountable. With proper resources, this initiative could serve as a critical early-warning system against foreign influence and research fraud, verifying that federal funds are spent exactly as Congress intended. This would also ensure that the Agency is not solely relying on self-reporting by institutions.

---

[4] DOJ, "University of Delaware Failed to Disclose Professor's Foreign Government Ties," press release, December 16, 2024.

[5] U.S. Congress Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, *Research Security for America's Future in Space—NASA's Enforcement of the Wolf Amendment* (May 14, 2026).

Safeguarding Scientific Data Through Strict Cybersecurity Enforcement

NASA is continuing to expand its collaborative partnerships to drive scientific innovation, entrusting a wider network of contractors and grantees with access to sensitive data. As a result, securing government information and ensuring federal awardees comply with strict security standards remains a top priority for the OIG. When individuals or institutions disregard these critical requirements, they expose NASA's cutting-edge research to foreign adversaries.

In the early 1990s, NASA OIG was one of the first federal oversight agencies to establish its own Cyber Crimes Division (CCD), pursuing those who jeopardize the Agency's information systems. Initially, CCD's investigations primarily involved unauthorized access, intrusions, and data theft driven by relatively unsophisticated actors exploiting vulnerabilities in NASA's decentralized information technology (IT) environment. Over the last decade, as the Agency strengthened its cybersecurity posture and improved its centralized controls, our foreign adversaries also developed more advanced threat campaigns. Today, CCD counters complex cybercriminals backed by significant resources and funding, including state-sponsored groups, Advanced Persistent Threat actors, and highly organized criminal enterprises operating overseas. Because NASA contractors and grant recipients maintain privileged access to government systems, they offer a foothold for bad actors seeking to infiltrate Agency networks.

Cyber-enabled crimes can be extremely far-reaching and complex, disregarding international borders and affecting contracts and grants potentially worth billions of dollars across multiple agencies. As a result, NASA OIG frequently collaborates with federal partners to investigate institutions, researchers, and contractors that fail to comply with cybersecurity requirements.

CCD was one of the first members of the DOJ's Civil Cyber-Fraud Initiative, which identifies and dismantles emerging cyber threats to critical government data and infrastructure.[6] Under the FCA, the Initiative pursues individuals and entities that knowingly furnish deficient cybersecurity products or services, misrepresent their cybersecurity practices or protocols, or disregard their obligations to monitor and report breaches and incidents. Since this joint enforcement effort launched in 2021, the OIG has participated in 15 Civil Cyber-Fraud Initiative cases. The Initiative has strengthened interagency collaboration and fortified cybersecurity requirements across federal contracts, driving major awardees to adopt more robust IT security practices.

In one civil cyber fraud case, the Pennsylvania State University agreed to pay $1.25 million to resolve allegations that it violated the FCA by failing to comply with federal cybersecurity requirements.[7] Investigators determined that, between 2018 and 2023, the university did not implement cybersecurity controls required in 15 contracts and subcontracts involving NASA and the Department of War. In addition, Penn State did not adequately develop and implement plans to correct these vulnerabilities. Although the university did report its deficient cybersecurity scores to the War Department, the university misrepresented its timeline for compliance and never implemented the required controls.

---

[6] DOJ, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," press release, October 6, 2021.

[7] DOJ, "The Pennsylvania State University Agrees to Pay $1.25M to Resolve False Claims Act Allegations Relating to Non-Compliance with Contractual Cybersecurity Requirements," press release, October 22, 2024.

Investigations like this underscore the importance of cybersecurity oversight and highlight the critical role civil fraud enforcement plays in defending NASA's interests. When institutions neglect federal requirements, it is a breach of both public trust and national security.

Maximizing Recoveries Through Timely and Proactive Investigations

Conducting timely and proactive investigations to recoup misspent funds from those who violate the FCA is another top priority for the OIG. If funds are recovered while an appropriations account is still open, amounts that constitute reimbursements or refunds for ill-gotten gains are returned directly to NASA. In other circumstances, the money reverts to the U.S. Treasury, such as when the relevant appropriations account has closed or the recovered monies exceed a reimbursement, as in the case of double or treble damages.

The OIG's ongoing, proactive initiatives leverage data analytics and other intelligence tools to identify and investigate issues related to the compromise of sensitive NASA information. Over the last decade, the OIG has initiated nearly 400 proactive projects, with a total monetary impact of over $93 million and almost $30 million recovered for NASA. These projects also generate critical leads, seeding numerous derivative investigations into previously undetected vulnerabilities. For example, the OIG routinely collaborates with federal partners to expose individuals across agencies who are attempting to exfiltrate knowledge and technology to foreign entities. In addition to detecting foreign interference, these joint efforts facilitate intelligence sharing and broad industry outreach, enabling timely threat identification.

As another preemptive measure, the OIG has partnered with the Agency's Science Mission Directorate to develop a software tool that identifies and provides risk scoring for NASA researchers with potential affiliations or research publications tied to China. The OIG's specialized intelligence and threat analysis unit is also devising its own tool to acquire and evaluate open source information and augment investigations. These data-driven approaches increase efficiency by allowing the OIG to focus time and resources on high impact cases where criminal and civil prosecutions are most likely.

Our proposed site visit initiative will serve as the next phase of this proactive oversight model, amplifying our early-warning capabilities across the Agency. By delivering rapid, actionable recommendations to NASA leadership, we can swiftly close security gaps and deny foreign adversaries access to sensitive Agency data. In addition, the OIG is collaborating closely with Agency leadership to enforce strict access controls across NASA's physical facilities and IT systems. This ongoing effort ensures that only fully vetted personnel maintain access to critical infrastructure, closing potential entry points for malicious actors.

Because the integrity of federally funded research depends upon truthful representations to the government, timely oversight is paramount to intercepting grant fraud before foreign entities can exploit NASA's vulnerabilities.

Conclusion

As NASA's investments in scientific innovation continue to grow, it is critical that the Agency acknowledge and close existing gaps in its research security posture. To that end, Agency officials are currently engaged with our office as we pursue policy updates and other efforts to enforce stricter oversight of grants and contracts.

In addition, the Agency has established a dedicated research security office and shown willingness to update its award terms and conditions, enhance disclosure requirements, and explore more robust post-award monitoring frameworks. This responsiveness affirms NASA's commitment to addressing vulnerabilities that leave scientific advancements unprotected. Nonetheless, without stronger controls, notable weaknesses will persist and heighten the risk of foreign influence and research fraud.

We look forward to continuing our collaboration with NASA and Congress to execute the aggressive oversight needed to fight fraud and strengthen accountability, transparency, and research integrity as America continues its journey back to the Moon and on to Mars.