Statement of Kelly P. Mayo
Deputy Inspector General for Investigations
Department of Defense Office of Inspector General
Before the House Oversight Subcommittee on Government Operations
June 4, 2025
Hearing on "Safeguarding Procurement: Examining Fraud Risk Management in the Department of Defense"

Introduction

Chairman Sessions, Ranking Member Mfume, and Members of the Subcommittee:

Thank you for the opportunity to testify today regarding the important topic of procurement fraud in the Department of Defense (DoD).

As the Deputy Inspector General for Investigations, I lead the Defense Criminal Investigative Service (DCIS), the criminal investigative arm of the DoD Office of Inspector General (DoD OIG). My testimony reflects the experience of hundreds of special agents, analysts, and support staff working to expose fraud and protect the integrity of U.S. defense spending at home and abroad.

Procurement fraud is not only a financial issue—it is a national security concern. Every act of deception, whether through bribery, product substitution, or false billing, harms the readiness and effectiveness of the Department. When warfighters rely on systems compromised by greed or mismanagement, the consequences are operational, strategic, and human.

Combating this threat requires more than internal vigilance; it demands a unified national response. To protect DoD procurement processes and uphold the integrity of the nation's defense infrastructure, we must have the full engagement and support of Congress. This important effort is not just about safeguarding budgets,— it is about protecting the men and women who serve and maintain the credibility of our national defense apparatus.

Historical Perspective

DCIS was formed in the early 1980s in response to a series of procurement scandals that shook public confidence in military spending. At the time, headlines captured the public's attention with stories of overpriced hammers and mismanaged contracts. But the problem was deeper than anecdotal excess. DCIS investigations revealed a pattern of corruption, lack of oversight, and collusion that eroded the integrity of the entire defense procurement process.

In response, Congress created structural safeguards. The DoD OIG was given broad investigative and audit authorities, and DCIS was tasked with enforcing the law across the Department's massive acquisition system. In the decades since, DCIS investigations have led to the prosecution of hundreds of subjects, recovered billions in fraudulently obtained funds, and helped shape defense procurement reform. And yet, as fraud schemes have become more sophisticated, and as the scale of defense spending has surged, our challenge has grown in kind.

The Scale and Complexity of DoD Procurement

Today, the DoD obligates more money through contracts than all other Federal agencies combined. The DoD's budget is approximately $850 billion for FY 2025, and a significant amount will be allocated through an acquisition system that comprises thousands of vendors and spans the globe.

This scope is not inherently problematic. In fact, it reflects the ambition and complexity of U.S. defense strategy. But it also creates a rich environment for exploitation. Where complexity exists, so too does the opportunity for concealment. Where oversight is thin, fraud flourishes.

Fraudsters—both individuals and corporations—understand this dynamic. They exploit it through product substitution, overbilling, rigged bids, falsified quality testing, and illegal coordination among supposed competitors. They operate domestically and internationally. They use encrypted communications, shell corporations, and digital obfuscation. Some work alone; others are part of coordinated networks. The frauds vary in method, but their impact is consistent: weakened systems, wasted resources, and compromised trust.

Types of Fraud Affecting the DoD

While no two fraudulent enterprises are entirely alike, DCIS continuously encounters schemes involving the following types of fraud.

- Product Substitution and Counterfeit Products: Numerous DCIS investigations have revealed contractors delivering counterfeit or substandard products while falsely certifying compliance with military specifications. A single substituted part, such as an inferior connector in a missile guidance system, can result in catastrophic failure.
- Cost Mischarging and Defective Pricing: Some contractors shift costs improperly from fixed-price to cost-reimbursable contracts or misrepresent their cost structure

to inflate pricing. These practices violate the Truth in Negotiations Act and have led to major recoveries.

- Bribery and Public Corruption: We have investigated officials who exchanged contract awards for gifts, cash, or employment. These cases erode fairness and increase the likelihood of unqualified vendors receiving critical work.
- Cybersecurity and False Certifications: Contractors have falsely claimed compliance with cybersecurity standards, placing sensitive DoD data at risk. One recent investigation led to a $4.6 million settlement after a company falsely attested to protecting controlled unclassified information.
- Export Control Violations: We have arrested individuals attempting to transfer controlled defense technology to adversarial states. These efforts often involve front companies and covert networks.

Real Case Illustrations

The following list summarizes a few recent criminal investigations that exemplify the nature and stakes of DoD procurement fraud.

- Raytheon (2024): Agreed to pay over $950 million to resolve allegations involving defective pricing, bribery, and export control violations. The case involved false cost representations and unauthorized exports of sensitive technologies to restricted regions.
- MORSE Corp. (2025): Paid $4.6 million due to cybersecurity fraud. Investigators determined that the company had grossly overstated its compliance with

government-mandated cybersecurity protocols while competing for contracts involving sensitive systems.

- Aventura Technologies (2024): Pleaded guilty to wire fraud after misrepresenting Chinese-made components as U.S.-origin. The components were installed in systems used across DoD installations—raising significant concerns over operational integrity and data security.
- Leonard Glenn Francis (2024): Also known as "Fat Leonard," he orchestrated a vast bribery network that compromised Navy contracting operations across the Pacific. His case, one of the most consequential in Naval history, exposed a culture of complicity and underscored the risks of long-term contractor fraud.

Global Operations and Emerging Threats

In response to an increasingly globalized and complex threat environment, DCIS has expanded its operational footprint to safeguard U.S. interests beyond national borders. DCIS special agents are now stationed abroad in strategic locations, working in close coordination with State Department officials, defense attachés, and host nation law enforcement. These forward-deployed teams investigate fraud, corruption, and illicit networks that threaten the integrity of international security assistance programs and act as a deterrent to those who may seek to misuse U.S. resources. For example:

- In Ukraine, DCIS is working with local anti-corruption authorities and other Federal agencies to monitor the end-use of U.S. weapons and equipment and investigate allegations of diversion.
- In Southwest Asia, DCIS is investigating fraud schemes involving or impacting the military's strategic deterrence activities in Qatar, Kuwait, and Bahrain.

- In the Indo-Pacific region, DCIS is pursuing multiple investigations involving procurement fraud and cyber-enabled intrusions. As U.S. defense posture increases in the region, so too do attempts to exploit contracting vulnerabilities, especially around base services and infrastructure projects.

The Importance of Interagency Coordination

Interagency coordination is not just a component of our mission. It is a force multiplier in the fight against procurement fraud and national security threats. DCIS is proud to serve as a trusted partner to more than 60 Federal, State, and international agencies, including the Department of Justice, Federal Bureau of Investigation, Homeland Security Investigations, and all branches of the military's criminal investigative organizations. In the past year alone, we participated in more than 200 joint operations, bringing our unique expertise in defense procurement and contractor fraud into some of the nation's most complex and high-impact investigations.

These collaborations are operationally decisive. Together, we have dismantled global fraud networks, uncovered schemes that compromised military readiness, and recovered hundreds of millions of dollars for taxpayers. By aligning investigative resources, sharing intelligence, and pursuing coordinated enforcement actions, we not only increase efficiency—we amplify deterrence. This unified approach ensures that those who seek to exploit the defense enterprise face coordinated and uncompromising accountability.

Barriers to Combating Fraud

Several systemic challenges limit our effectiveness.

- Lack of Centralized Contract Data: Many DoD contracting elements do not input full bid or pricing information into searchable databases. This impairs our ability to use data analytics and artificial intelligence tools to proactively detect anomalies.

- No Visibility into Subcontractors: Prime contractors are not required to disclose full subcontractor rosters. Fraud often hides several tiers down the chain, so lack of subcontractor data makes it difficult to identify and investigate fraud schemes.
- Gaps in Export Control Access: DCIS lacks direct access to some critical records from the Directorate of Defense Trade Controls. This slows our work involving counterproliferation.
- Use of Commercial Item Exemptions: Contractors may assert that items are "commercial," exempting them from providing certified cost or pricing data to DoD contracting officials. Without that data, we are unable to identify inflated costs.
- Jurisdictional and Legal Complexity: The globalization of all white-collar crimes, including procurement fraud, has resulted in significant challenges. Investigating procurement fraud often involves navigating multiple legal systems, differing definitions of criminal conduct, and conflicting privacy or data protection laws, making evidence collection and prosecution significantly more difficult.

Investigators as Force Multipliers

Despite these obstacles, the return on investment from DCIS operations is, to say the least, remarkable—more than $3 billion in the last fiscal year and accomplished with only 381 Federal agents. This statistic equates to an astonishing return on investment but does not take into account deterrence or the operational value of preventing a mission-critical failure due to fraud.

We fully recognize the constraints on Federal resources and the responsibility we bear as stewards of taxpayer dollars. Accordingly, we are committed to constantly refining our processes to improve efficiency, enhance recovery efforts, and strengthen support to partner agencies and DoD Components.

Conclusion

In conclusion, procurement fraud is not a technical irregularity for the DoD. It is a strategic vulnerability that siphons taxpayer funds and undermines public trust.

For more than four decades, DCIS has aggressively targeted fraudsters. We take great pride in the fact that everything we do is in service to the warfighter. Fraud compromises readiness, hinders morale, and, in the worst cases, can be lethal. Our investigations have removed counterfeit aircraft components, untested medical devices, and falsified maintenance logs from use in operational theaters. We have stopped threats before they reached the battlefield.

Our role in DCIS is to remove corruption, recover stolen resources, and ensure that our military receives what it pays for honestly, reliably, and on time. We remain unwavering in our mission to safeguard the integrity of the DoD procurement process. Ongoing engagement and support from Congress are essential to reinforcing this mission and upholding the trust placed in us by the American people and those who serve. We look forward to working in a continued partnership with this subcommittee to uphold the standards our warfighters and taxpayers deserve.

Thank you for your continued support of the DoD OIG's mission to conduct independent oversight of the DoD. I welcome your questions.