RESTON

The Risks of Playing Through the Whistle:

Whistleblowers, the False Claims Act, and the DOJ's Expanding Civil Cyber-Fraud Initiative

Bruce C. Judge | **Whistleblower Law Collaborative LLC**

2025

www.cs2.cloud/reston

Bruce C. Judge

Bruce C. Judge

Member of the Whistleblower Law Collaborative LLC

Bruce Judge is a member of the Whistleblower Law Collaborative (WLC) based in Boston, Massachusetts. Prior to helping launch WLC, Bruce spent 23 years as prosecutor with the Department of Justice, investigating, charging, and trying individuals and companies for financial crimes, obstruction of justice, public corruption, and other federal offenses.

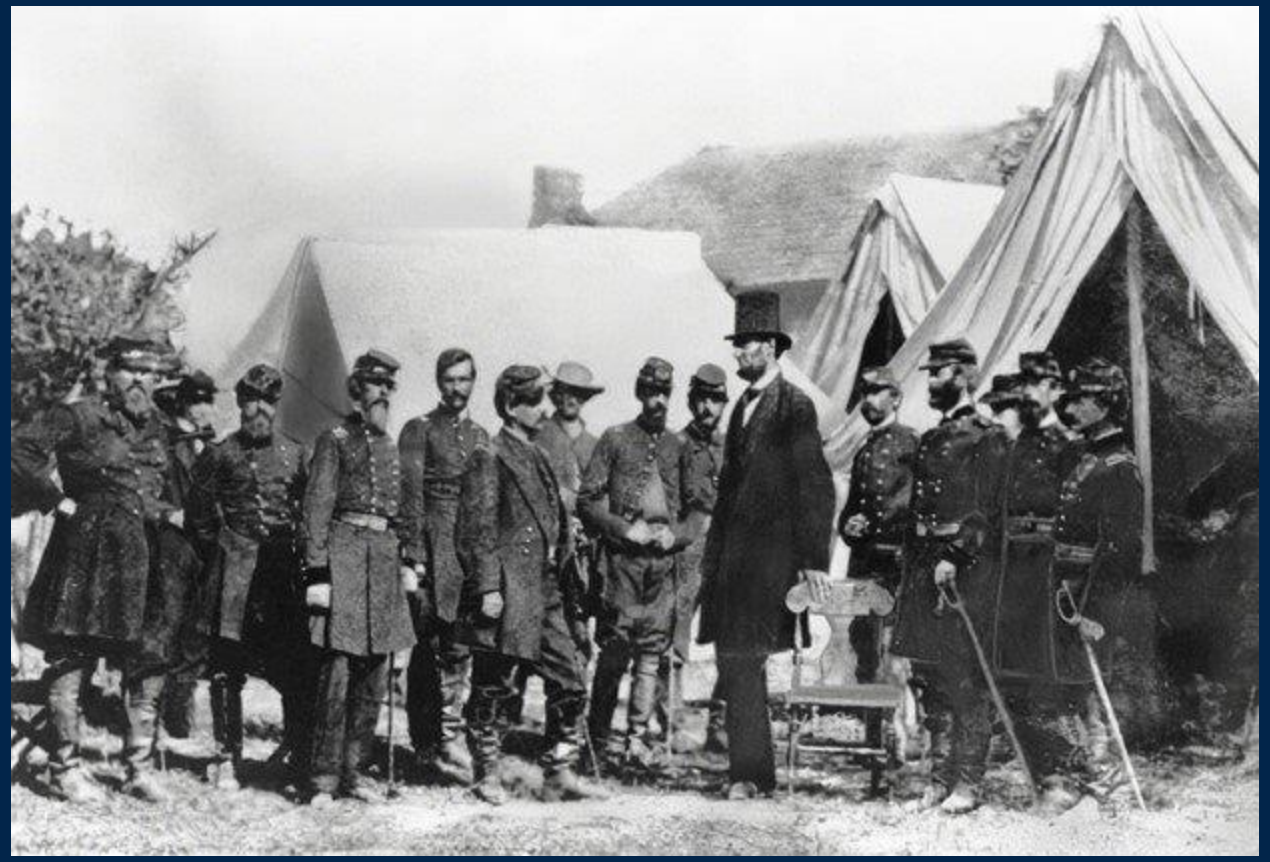
Bruce is a regular presenter at legal conferences and law enforcement training sessions.

In October 2024, Bruce was a member of a panel convened by the Federal Bar Association to discuss lessons learned during the first three years of DOJ's Civil Cyber-Fraud Initiative. The same panel included the DOJ attorney who supervises the Civil Cyber-Fraud Initiative and one of the attorneys who represented Aerojet Rocketdyne in the FCA lawsuit which resulted in a $9M settlement.

In February 2025, Bruce made a half-day presentation to the Council of Inspector Generals in Washington DC on best practices for federal agents conducting investigations based on tips received from private citizen whistleblowers.

Bruce was one of the attorneys representing the Relator in the Morse case. The first FCA settlement with a Defense Contractor/Member of the DIB for failing to implement cybersecurity requirements – specifically the controls in NIST SP 800-171 – as required by its contracts with the Department of the Army and the Department of the Air Force.

“Lincoln’s Law”



“Qui Tam” Provisions

- “Qui tam pro domino rege quam pro se ipso in hac parte sequitur”
- Concept borrowed from Middle Ages in England
- Private citizens could bring actions as private prosecutors in the name of the king and get a bounty if successful.

Original FCA – Two Fundamental Goals

- **Punish fraud**
  - **Double damages and $2,000 fine for each false claim**
- **Incentivize Whistleblowers**
  - **Relator's share 50% of recovery**

1943-1986 FCA was weakened

Congress nearly abolished FCA during WWII

Kept but drastically weakened

- **Response to "parasitic" lawsuits**
- **Reduced incentives for whistleblowers (0-25%)**
- **Barred qui tam cases if government already had information**

Fraud, Waste & Abuse Exposed

$640

$436

1986 Amendments - Modern-Day FCA

- **Bipartisan legislation**
- **Signed into law by President Reagan**

What did amendments do?

INCREASED INCENTIVES FOR WHISTLEBLOWERS

MADE IT EASIER TO PUNISH FRAUD

“Going after waste, fraud, and abuse without whistleblowers is about as useful as harvesting acres of corn with a pair of rusty old scissors.”

Senator Charles Grassley, Chairman of Senate Judiciary Committee, speech given on National Whistleblower Day (July 30, 2018).

INCREASED Incentives for Whistleblowers

Successful whistleblowers entitled to 15-30% of government's recovery

"Government knowledge" bar relaxed
- Information must be *publicly* disclosed
- If whistleblower is "original source" of the information, not barred

Retaliation Protection for Whistleblowers

Defendants liable for payment of successful relator's attorneys' fees

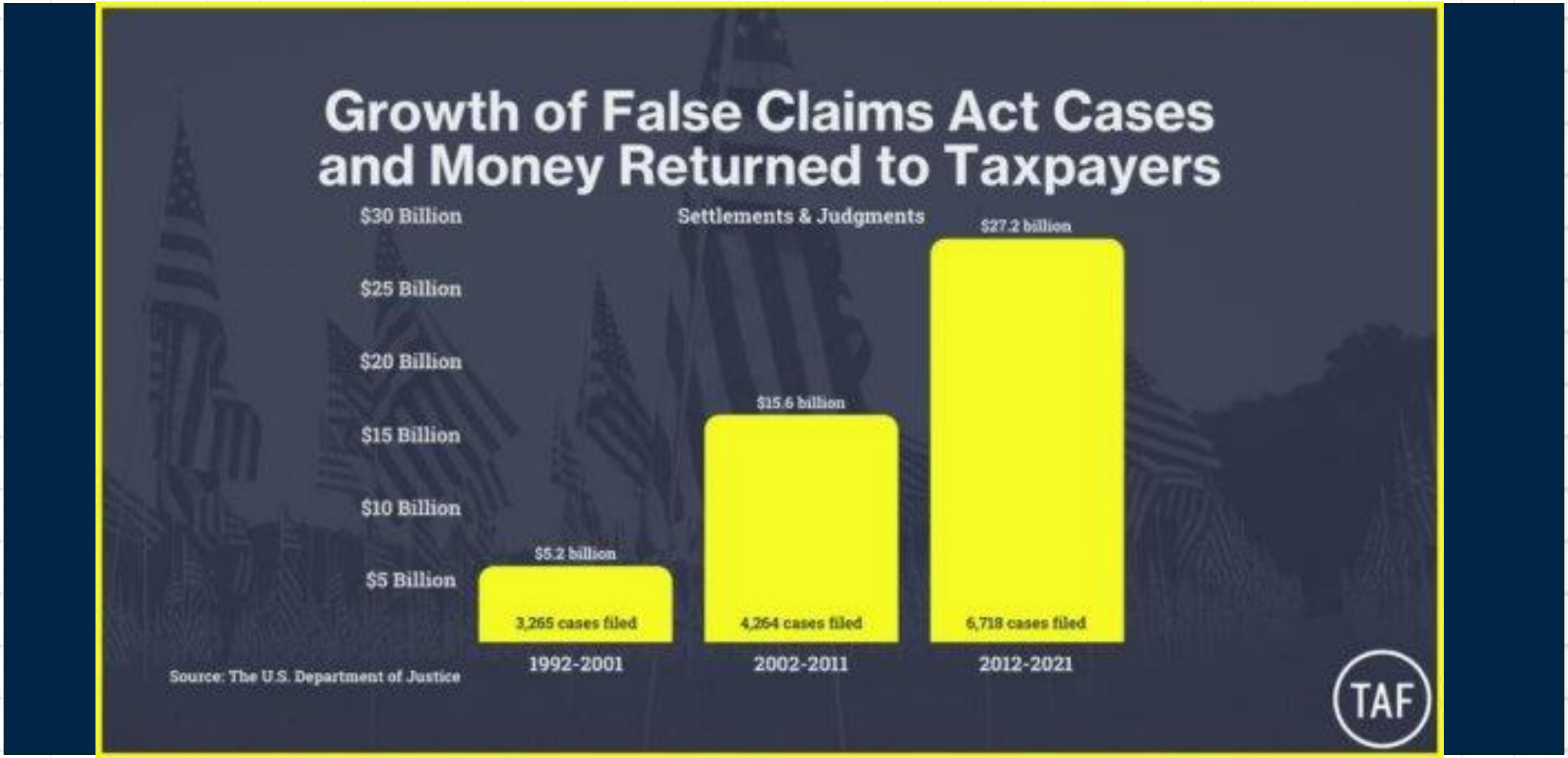
Punishing Wrongdoers

- **Easier to prove fraud – expansive definition of "knowledge"**
  - **"actual knowledge"**
  - **"deliberate indifference"**
  - **"conscious avoidance"**
- **Greater consequences for defendants**
  - **Damages – treble damages**
  - **Penalties – currently $13,508 – $27,018 per claim**
  - **Attorneys' fees**

Result of 1986 Amendments

- More resources
- More whistleblowers
- More cases prosecuted
- More money collected from defendants
- More money paid to whistleblowers

DOJ Statistics – Qui Tam Cases



THE FALSE CLAIMS ACT HAS BROAD REACH

TAF

FCA Process

- Complaint filed under seal
- Mandatory Disclosure and evidence served on the U.S. Attorney
- Government investigates while case remains under seal (at least 60 days but likely several years)
- Case Unsealed
- Notice of Intervention or Declination or Settlement

31 U.S.C. 3729(a)(1)

A. knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval;

B. knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim;

C. conspires to commit a violation of subparagraph (A-G)

…

G. make, use or cause to be made or used a false record or statement material to an obligation to pay or knowingly conceal or knowingly and improperly avoid or decrease an obligation

Scienter/Knowledge

Georgia Tech Complaint-in-Intervention:

- Awareness of Non-Compliance
- Deliberate Ignorance or Reckless Disregard
- Continued billing despite knowledge
- Failure to report breaches

United States ex rel. Craig v. Georgia Tech Research Corp., et al., No. 1:22-cv-02698 (N.D. Ga.)

Materiality

Georgia Tech Complaint-in-Intervention:

- Compliance with NIST standards is a material condition of payment
- Misrepresentations of Quality and Content is material
- Fulfilling contract requirements is material condition of payment
- Would not have paid if known about Georgia Tech's non-compliance

United States ex rel. Craig v. Georgia Tech Research Corp., et al., No. 1:22-cv-02698 (N.D. Ga.)

Recovery/Penalties

- Treble damages (actual losses x 3)
- Penalty per claim (currently $13,946 to $27,894)
- Whistleblower’s expenses, costs, and attorney’s fees

Whistleblower Reward | "Relator's Share"

- Intervention 15%-25%
- Declination 25%-30%
- Exceptions

Retaliation

- The FCA (and many separate state laws) provide the ability for a relator to file a separate claim, personal to themselves, for retaliation suffered due to any “lawful acts” taken “in furtherance of” an FCA action

- This claim is personal to the relator, the government has no stake in it

- Defendants may be liable for ‘black-balling’ former employees

Frivolous Suits

- The FCA permits a defendant to recover its reasonable attorneys' fees, expenses, and costs if:

(1) the defendant prevails in the action and

(2) the court finds that the claim of the person bringing the action was clearly frivolous, clearly vexatious or brought primarily for purposes of harassment.

- Usually when the government declines and the Relator pushes ahead with full litigation.

DOJ’s Civil Cyber-Fraud Initiative

For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it. Well that changes today.

We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk.

-Deputy Attorney General Lisa O. Monaco when announcing the initiative in 2021.

How DOJ CCFI may calculate damages

- Value of contracts cannot be ruled out
- Credit given for self-reporting – Verizon was given credit for self-reporting its cybersecurity failures

Other “Cyber” Settlements

- Guidehouse, Inc./Nan McKay $11.3 million
- Verizon $4 million
- Penn State $1.25 million
- Jelly Bean Communications $293,771

MORSECORP Inc. $4.6 Million Settlement

- Used a third party company to host emails without confirming the company met FedRamp security requirements

- Failed to implement NIST SP 800-171 Cybersecurity Controls

Office of Public Affairs | Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations | United States Department of Justice

MORSECORP continued

- Failed to fully implement System Security Plan for covered information systems
- Posted inaccurate SPRS score and failed to update

MORSECORP continued

"Federal contractors must fulfill their obligations to protect sensitive government information from cyber threats. We will continue to hold contractors to their commitments to follow cybersecurity standards to ensure that federal agencies and taxpayers get what they paid for, and make sure that contractors who follow the rules are not at a competitive disadvantage."

- U.S. Attorney Leah B. Foley for the District of Massachusetts

MORSECORP continued

“Protecting the integrity of Department of Defense (DoD) procurement activities is a top priority for the DoD Office of Inspector General’s Defense Criminal Investigative Service (DCIS). Failing to comply with DoD contract specifications and cybersecurity requirements puts DoD information and programs at risk. We will continue to work with our law enforcement partners and the Department of Justice to investigate allegations of false claims on DoD contracts.”

- Special Agent in Charge PatrickJ. Hegarty of the DCIS Northeast Field Office.

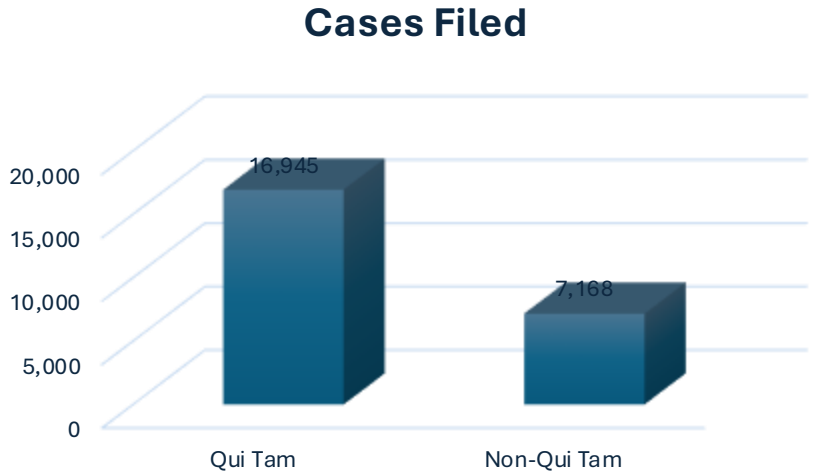
Georgia Tech Case Allegations

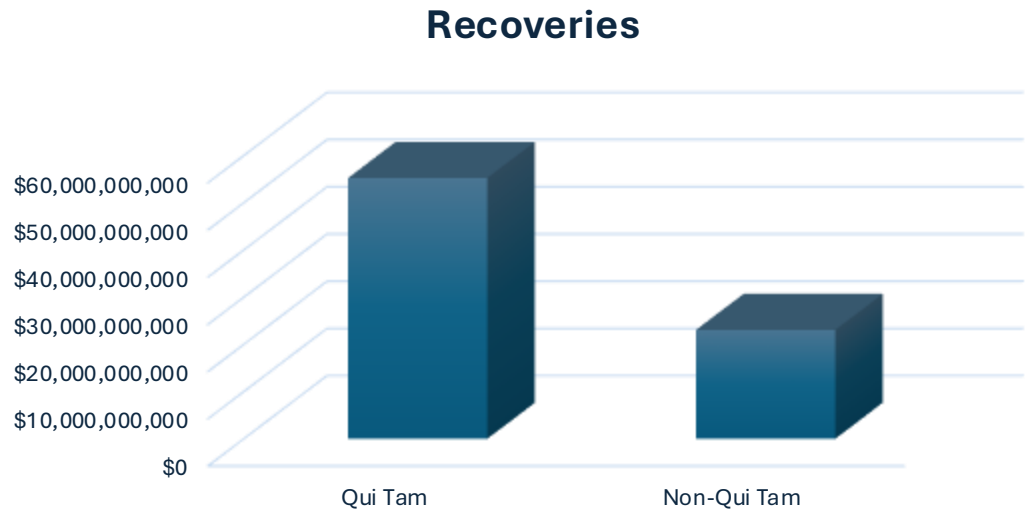
- Failure to develop and implement a System Security Plan (SSP)
- Improper scoping of SSP
- Failure to install and maintain Anti-Virus/Anti-Malware software
- Submission of a false SPRS score
- “culture” of cybersecurity non-compliance

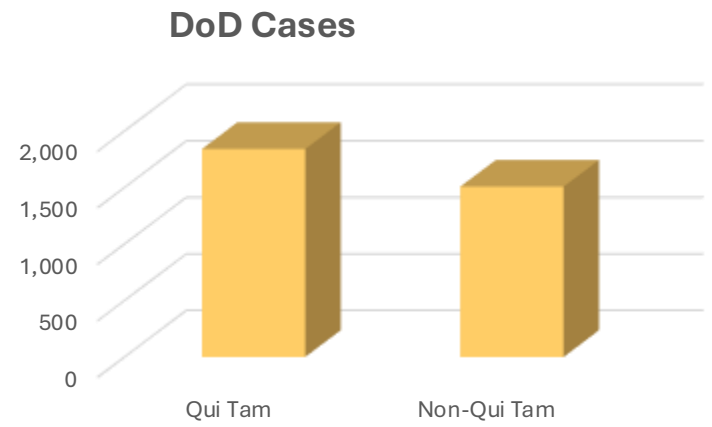
United States ex rel. Craig v. Georgia Tech Research Corp., et al., No. 1:22-cv-02698 (N.D. Ga.)

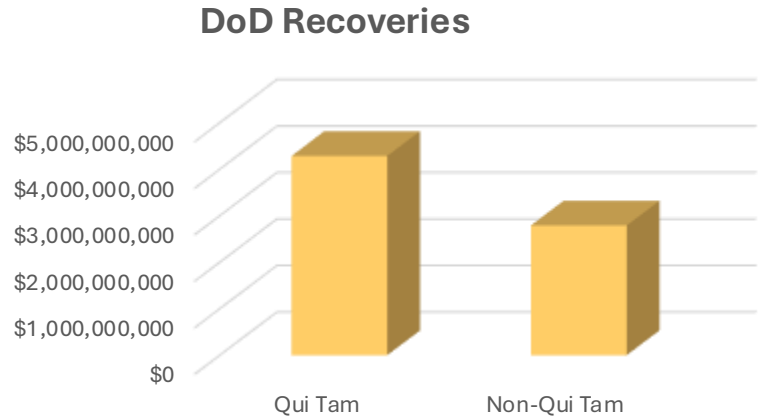
A cyber intrusion is not required for CCFI liability to attach.

DOJ Statistics – Totals from 1986 to Sept. 2024









https://www.justice.gov/archives/opa/media/1384546/dl

Other Cybersecurity Initiatives

U.S. Securities and Exchange Commission

- Mandatory disclosure of cybersecurity incidents – 4 business days
- Annual disclosure of cybersecurity risk management, strategy, and governance
- Board of directors should be actively involved in the oversight and management of cybersecurity risk
- Cybersecurity risk management integrated into overall enterprise risk management

https://www.sec.gov/files/33-11216-fact-sheet.pdf

NY DFS guidance on cyber risks and strategies

- Develop a Comprehensive Cybersecurity Policy
- Perform Periodic Risk Assessments
- Implement Technical Security Controls
- Appoint a Chief Information Security Officer (CISO)
- Develop an Incident Response Plan
- Train Your Cybersecurity Personnel

NEW YORK STATE OF OPPORTUNITY. | Department of Financial Services

Proposed FAR CUI Rule

On Jan. 15, 2025, the Department of Defense (DoD), General Services Administration, and NASA, all members of the FAR Council, published a proposed FAR CUI Rule under Title 48 of the CFR.

This proposed rule amends the Federal Acquisition Regulation (FAR) to implement the third and final piece of the National Archives and Records Administration's (NARA) Federal Controlled Unclassified Information (CUI) Program.

Just how do QT lawyers evaluate cases?

… Or how do QT lawyers screen clients?

How Qui Tam Lawyers Evaluate Cases

- What is the nature of the fraud?
- Do you have personal, non-public information about the fraud?
- Does it involve government-funded programs or contracts?

Continued

- What is the value of the fraud/contracts?
- Do you have documents or other evidence to corroborate the allegations?
- Does the fraud negatively impact public safety or patient care?

Potential Cyber-Fraud Cases

- Who are the government customers?
- Are there national security considerations?
- Does the company access, store, and process Controlled Unclassified Information (CUI)?

CCFI continued

- Where is the CUI located? Who has access?
- Is the company using cloud-based services that are not FedRAMP compliant?
- Is the company using GCC High versions of Teams and other cloud services?

CCFI continued

- Does the company have a valid System Security Plan (SSP)?
- When did the company last post a SPRS score?
- Was the score accurate?

CCFI Continued

- What NIST SP 800-171 controls are not being met?
- Are there POAMs in place? Is the company working to complete them?
- Does the company use Managed Service Providers (MSPs) or Managed Security Service Providers (MSSPs)? If so, are they foreign nationals and/or located offshore?

NDAA Section 883 (FY2021 NDAA)

Prohibits DoD from awarding a contract to a contractor that requires its employees to sign a confidentiality agreement "that would prohibit or otherwise restrict such employees from **lawfully reporting** waste, fraud, or abuse related to the performance of a Department of Defense contract to a designated investigative or law enforcement representative of the Department of Defense authorized to receive such information."

Requires DoD contractors to inform their employees of their right to lawfully report waste, fraud, abuse, and other wrongdoing.

Senator Grassley's annual appropriations rider bars federal contractors from enforcing gag clauses

Subpart 203.9
Whistleblower Protections for Contractor Employees

10 U.S.C. 4701 prohibits contractors and subcontractors from discharging, demoting, or otherwise discriminating against an employee as a reprisal for disclosing, to any of the entities listed at paragraph (3) of this section, information that the employee reasonably believes is evidence of …a violation of law, rule, or regulation related to a DoD contract…or a substantial and specific danger to public health or safety.

If You're in a Hole

- Maintain all records and communications
- Evaluate self-reporting options
- Consult experienced FCA Counsel

Questions?

Bruce C. Judge
Member | Whistleblower Law Collaborative LLC
20 Park Plaza, Suite 438 | Boston, MA 02116-4334
617.366.2800 main | 617.245.8185 direct