

THE WHISTLEBLOWER ADVOCATES

Qui Tam & Whistleblower Law Firm

The Complete Guide to Cybersecurity Whistleblowing

Under the False Claims Act | 2025-2026 Edition

For government contractors, IT professionals, compliance officers, and anyone with knowledge of cybersecurity fraud against the U.S. government.

FREE CONFIDENTIAL CONSULTATION

(833) 310-3147

thewhistlebloweradvocates.com

Important Legal Notice

This guide is provided for general informational and educational purposes only. It does not constitute legal advice and does not create an attorney-client relationship. The law governing False Claims Act qui tam actions and whistleblower protections is complex and fact-specific. Every case is different.

If you believe you have knowledge of cybersecurity fraud against the U.S. government, you should consult with a qualified whistleblower attorney before taking any action, including gathering additional evidence, speaking with colleagues, or contacting the government directly.

The Whistleblower Advocates offers free, confidential consultations. Nothing you share in a consultation is disclosed without your consent. Call (833) 310-3147 or visit thewhistlebloweradvocates.com.

CRITICAL: Do not collect evidence without first speaking to an attorney.

How you obtain evidence matters enormously. Accessing systems you are not authorized to use, or taking documents in a manner that violates company policy or computer fraud laws, can jeopardize your case and expose you to liability. An experienced whistleblower attorney will guide you on how to preserve what you already have — legally.

Section 1: What Is Cybersecurity Fraud Against the Government?

Not every cybersecurity failure is fraud. A genuine misconfiguration, an honest compliance gap, or a good-faith disagreement about a technical control does not create a False Claims Act case. What does create a case is when a company knowingly misrepresents its cybersecurity posture to the federal government — and receives taxpayer money as a result.

The False Claims Act (FCA) makes it unlawful to submit a false or fraudulent claim to the U.S. government. In the cybersecurity context, that fraud most often takes one of three forms:

1. Certifying compliance with requirements the company never implemented

Every year, thousands of defense contractors and federal vendors sign contracts that include cybersecurity requirements as conditions of payment. When a company checks the box on a compliance certification — DFARS, CMMC, FedRAMP, or others — without actually meeting the underlying requirements, that certification becomes a false claim.

2. Falsifying the SPRS Score

The Supplier Performance Risk System (SPRS) requires contractors to self-assess their implementation of NIST SP 800-171 security controls and submit a score to the Department of Defense. A perfect score is 110. Most companies fall short. The fraud occurs when a contractor submits an inflated score — reporting 95 when the honest score is 30, for example — in order to appear compliant and win or retain government contracts.

This is one of the most common and actionable forms of cybersecurity fraud. A whistleblower who can document the gap between a submitted SPRS score and the company's actual security posture has a potentially strong FCA claim.

3. Failing to report cybersecurity incidents as required

DFARS 252.204-7012 requires contractors to report cyber incidents affecting covered systems within 72 hours of discovery. Companies that discover breaches and bury them — or that fail to implement the required incident reporting capabilities at all — may be submitting false claims each time they certify compliance and accept payment.

Framework	What It Requires — and Where the Fraud Happens
DFARS 252.204-7012	Contractors handling Covered Defense Information (CDI) must implement NIST SP 800-171 controls and report cyber incidents within 72 hours. Fraud: certifying compliance without implementing controls; failure to report breaches.
DFARS 252.204-7019	Contractors must conduct a NIST 800-171 self-assessment, calculate an accurate SPRS score, and submit it to DoD prior to contract award. Fraud: submitting inflated scores; using stale or fabricated assessments.
CMMC 2.0	DoD contractors at Level 2+ must be assessed by a certified third-party (C3PAO). Fraud: bribing or colluding with assessors; falsely certifying controls not in place; assessors certifying non-compliant contractors.
NIST SP 800-171	110 security controls for protecting Controlled Unclassified Information (CUI). Fraud: attesting to implementing controls that exist only on paper; using a fake System Security Plan (SSP).
FedRAMP	Cloud service providers serving federal agencies must obtain FedRAMP authorization. Fraud: marketing services as FedRAMP authorized without completing the process; maintaining authorization while allowing controls to lapse.
ITAR / EAR	Controls on defense technology exports. Note: ITAR violations are reported through a separate process (State Dept. DDTC) — not via FCA qui tam. Consult an attorney to understand the right channel.

The DOJ Cyber Fraud Initiative — Why Now

In October 2021, the U.S. Department of Justice launched the Civil Cyber-Fraud Initiative (CCFI), formally deploying the False Claims Act as the government's primary enforcement tool for cybersecurity fraud by contractors and grantees. Since then, the DOJ has pursued cases against Aerojet Rocketdyne, Penn State University, Insight Global, and Raytheon/Nightwing, among others. This initiative is active, well-funded, and accelerating. The government has made clear: cybersecurity compliance is not optional, and the FCA is the tool it will use to enforce it.

Section 2: Do You Have a Case? A Self-Assessment Checklist

Before calling an attorney, it helps to understand whether your situation contains the core elements of an FCA cybersecurity claim. This checklist is not a legal opinion — it is a starting point for your thinking. A qualified attorney will evaluate your specific facts in detail.

The three core elements of an FCA cybersecurity claim:

1. A false or fraudulent statement or certification
2. Made knowingly (not just negligently)
3. That was material to the government's decision to pay

Ask yourself these seven questions:

- 1. Does your employer hold federal contracts or receive federal funding — including grants, loans, or reimbursements from agencies like DoD, HHS, or DHS?

If yes, the FCA applies. Cybersecurity fraud is not limited to defense contractors. Healthcare IT vendors, universities, research institutions, and any entity that certifies compliance to receive federal money may qualify.

- 2. Has your employer represented to the government that it meets specific cybersecurity requirements — in a contract, in a certification, or in a compliance submission?

This includes signing contracts with DFARS clauses, submitting SPRS scores, achieving CMMC certification, or attesting to FedRAMP compliance. If there is a representation of compliance, there is a potential false claim.

- 3. Do you have firsthand knowledge — not just suspicion — that those representations are false?

The FCA requires original-source knowledge. You don't need a complete audit trail, but you need to know something specific: a control that was faked, a score that was inflated, a breach that was concealed. Rumors and guesses generally aren't enough.

- 4. Is the non-compliance knowing — meaning did someone in management understand the gap and choose not to fix it, or actively misrepresent it?

This is the knowledge element that separates fraud from negligence. If your IT team flagged a gap, was told to close it, documented the risk, and the company kept certifying compliance anyway — that pattern is evidence of knowing fraud. Emails, internal audit reports, risk assessments, and meeting notes all matter here.

- 5. Is your information original — meaning it isn't already public, and the government doesn't already know about it?

The FCA's 'public disclosure bar' limits qui tam suits based on information already in the public domain (government audits, news reports, court filings). If your knowledge is drawn from your own direct experience inside the company, you are likely the original source. An attorney can assess whether any public disclosure issue applies.

- 6. Do you have, or can you describe, documentation that supports your allegations?

The strongest cases have documentary support: emails showing management awareness of non-compliance, internal audit results showing real scores vs. submitted scores, a System Security Plan that is clearly fabricated, a breach report that was never filed. You don't need a perfect file — attorneys file cases with incomplete records and conduct discovery. But the more specific your knowledge, the stronger the starting position.

- 7. Are you the first person to file? The FCA rewards the first relator to file — if a competitor or former colleague has already filed on the same fraud, your recovery may be limited.

Speed matters in qui tam cases. If you have been sitting on this information for months while deciding what to do, the most important next step is calling an attorney — today, not next week.

If you answered yes to most of these questions:

You may have the basis for a strong qui tam claim. The next step is a confidential consultation with a whistleblower attorney — not gathering more documents, not talking to colleagues, and not contacting the government on your own. Call The Whistleblower Advocates at (833) 310-3147.

Section 3: How the FCA Qui Tam Process Works — Step by Step

The False Claims Act qui tam process has a specific structure that is unlike any other type of litigation. Understanding it in advance helps you set realistic expectations and make informed decisions at each stage.

Step 1 — Retain a whistleblower attorney (before doing anything else)

The most important decision you will make is choosing your attorney. FCA qui tam cases are highly technical and require an attorney with specific experience in False Claims Act litigation, not just a general litigator. Before you gather additional evidence, before you speak to a colleague, before you contact any government

agency — hire a lawyer.

At The Whistleblower Advocates, your initial consultation is free and completely confidential. Nothing you share creates any obligation, and nothing is disclosed without your consent.

Step 2 — Investigation and complaint drafting

Your attorney will work with you to understand the facts, evaluate the strength of your claim, and draft a formal complaint. The complaint lays out the fraud in detail — what was represented, what was actually true, and how the government was harmed. For cybersecurity cases, this typically involves documenting the specific controls that were missing, the certifications that were false, and the contract payments that resulted.

Step 3 — Filing under seal

The complaint is filed in federal court under seal, meaning it is kept confidential from the public — and from the defendant. Only the court and the Department of Justice have access to it at this stage. This seal period is critical: it protects you, allows the government to investigate, and prevents the target from destroying evidence.

Step 4 — Government investigation

Once the complaint is filed, the DOJ (and often the relevant agency's inspector general) conducts its own investigation. This typically involves reviewing documents, interviewing witnesses, and assessing whether the evidence supports intervention. In cybersecurity cases, the DOJ may engage technical experts to evaluate the claimed compliance gaps.

The seal period is initially set at 60 days but is almost always extended — cybersecurity cases commonly remain under seal for one to three years while the government investigates. This is normal and expected.

Step 5 — Government intervention decision

At the end of its investigation, the DOJ decides whether to intervene — meaning take over the case and prosecute it directly — or decline. This is one of the most consequential moments in the process.

- **Government intervenes:** The DOJ takes the lead. The defendant typically knows the case exists for the first time. Settlement negotiations often follow. Relator share in intervened cases is 15–25% of the government's recovery.
- **Government declines:** The relator (you, through your attorney) can still proceed independently. Many declined cases settle. Some go to trial. Relator share in declined cases is 25–30%. Declined does not mean weak — it often means the DOJ has limited resources and is prioritizing other matters.

Step 6 — Settlement or litigation

Most FCA cybersecurity cases resolve through settlement rather than trial. The DOJ has strong incentive to settle once it has intervened and established liability. Your attorney negotiates the relator share as part of the settlement, and you are entitled to reasonable attorneys' fees regardless of the outcome.

Step 7 — Relator share payment

After the government recovers funds through settlement or judgment, your share is paid out. The full range is 15–30% of the total recovery, depending on whether the government intervened, how substantial your contribution was, and other statutory factors.

Stage	Typical Timeline (Cybersecurity FCA Cases)
Initial consultation to complaint filing	4 – 12 weeks
Seal period / government investigation	1 – 3 years (sometimes longer)
Intervention decision	Issued at end of investigation
Settlement negotiations	6 – 18 months post-intervention
Relator share payment	Follows final settlement or judgment
Total timeline (typical)	3 – 6 years from filing

What if the government declines my case?

A declination is not the end. The Whistleblower Advocates has specific experience litigating complex declined cases — an important distinction, as many whistleblower attorneys do not. If the government declines, your case does not automatically disappear. The decision to proceed is made case by case, based on the strength of your evidence and the recoverable damages.

Section 4: The DOJ Cyber Fraud Initiative — Why the Enforcement Climate Matters Now

Before 2021, cybersecurity fraud prosecutions under the False Claims Act were rare. The DOJ treated cybersecurity compliance as a regulatory matter — something agencies enforced through audits and administrative penalties, not through the courts. That changed.

What the Civil Cyber-Fraud Initiative (CCFI) changed

In October 2021, Deputy Attorney General Lisa Monaco announced the launch of the Civil Cyber-Fraud Initiative, formally deploying the False Claims Act as the enforcement mechanism for cybersecurity fraud by government contractors, grant recipients, and other federal funding recipients. The CCFI made several things explicit:

- Cybersecurity non-compliance that is knowingly misrepresented to the government is FCA fraud — not just a regulatory violation.

- The DOJ will use qui tam relators as the primary investigative mechanism — meaning it is actively looking for insiders with knowledge.
- The FCA's treble damages and per-claim penalties make cybersecurity fraud cases high-stakes for defendants.
- The initiative covers not just defense contractors, but any recipient of federal funds who makes cybersecurity representations.

Notable cases since the CCFI launched

Case	Summary
Aerojet Rocketdyne (2023)	Settled for \$9 million after a whistleblower alleged the company falsely certified compliance with DFARS and NASA cybersecurity requirements. One of the first CCFI settlements — established the enforcement template.
Raytheon / Nightwing (2025)	\$8.4 million settlement. Raytheon failed to implement required cybersecurity controls, including a System Security Plan, on DoD contracts between 2015 and 2021. Whistleblower was a former Director of Engineering.
Penn State University (2024)	\$1.25 million settlement. Penn State allegedly failed to implement required cybersecurity controls in its DoD research contracts and failed to assess subcontractors' compliance — demonstrating that research institutions face the same exposure as defense primes.
Gen Digital / Symantec (2024)	\$55.1 million settlement in a GSA contract pricing fraud case — not a cybersecurity compliance case, but involving a major cybersecurity firm, demonstrating the government's willingness to pursue large settlements against well-known vendors.
Insight Global (2023)	Settled for \$2.7 million. Staffing firm mishandled personal health information during COVID-19 contact tracing contract — a non-defense example of cybersecurity-adjacent FCA liability.

These cases share a common pattern: an insider with direct knowledge, documented evidence of a gap between represented and actual compliance, and a qui tam attorney who understood how to navigate the FCA process. The CCFI has made the government a willing and capable partner in these cases.

CMMC Phase 2 is creating a new wave of exposure

The Cybersecurity Maturity Model Certification (CMMC) program entered Phase 2 in late 2024, requiring third-party assessments (C3PAOs) for thousands of DoD contractors. This is the first time most of these contractors have faced external validation of their cybersecurity claims. The first wave of assessments is producing the first wave of fraudulent certifications — contractors certifying compliance to win contracts, C3PAOs under pressure to pass clients, and subcontractors left entirely unassessed despite their primes' representations to DoD. This is a significant, emerging, and underserved area for whistleblower claims.

Section 5: How Much Can a Cybersecurity Whistleblower Receive?

One of the most common questions we hear is: is this worth it financially? The honest answer is: it can be significantly worth it — and understanding the math helps you evaluate your situation realistically.

The statutory relator share

Under the False Claims Act, a whistleblower who files a successful qui tam case is entitled to a share of the government's recovery:

- 15% to 25% if the government intervenes and takes over the case
- 25% to 30% if the government declines and the relator proceeds independently

What drives the recovery amount?

The government recovers treble damages — three times the actual loss — plus civil penalties of up to \$27,894 per false claim. In a cybersecurity context, each contract payment made while the contractor was falsely certifying compliance can be counted as a separate false claim.

If a contractor received \$50 million in DoD contract payments over three years while falsely certifying DFARS compliance, the theoretical damages exposure before the relator share is calculated is \$150 million in treble damages, plus per-claim penalties. Actual settlements are typically negotiated below maximum exposure, but the leverage is substantial.

Scenario	Illustrative Relator Share Range
\$8.4M settlement (Raytheon scale) — government intervenes	\$1.26M – \$2.1M relator share
\$9M settlement (Aerojet scale) — government intervenes	\$1.35M – \$2.25M relator share

Scenario	Illustrative Relator Share Range
\$25M settlement — government intervenes	\$3.75M – \$6.25M relator share
\$50M settlement — government intervenes	\$7.5M – \$12.5M relator share
\$10M settlement — government declines, relator proceeds	\$2.5M – \$3M relator share

These figures are illustrative — every case is different, and recovery depends on the strength of the evidence, the size of the fraud, the government's willingness to intervene, and other factors. No attorney can guarantee a specific outcome.

Attorneys' fees

Under the FCA, if your case succeeds, the defendant pays your reasonable attorneys' fees — separately from your relator share. This means your recovery is not reduced by legal costs in a successful case. If the case is unsuccessful, The Whistleblower Advocates works on contingency — you owe no attorneys' fees.

The first-to-file rule: timing directly affects your recovery

The FCA pays only the first relator to file a claim on a given fraud. If you have been aware of the misconduct for months and someone else files first — a former colleague, another whistleblower, even a competitor — you may lose your right to a share entirely. The cost of waiting is potentially the entire recovery. Call us before you wait any longer.

Section 6: Protecting Yourself — Whistleblower Rights and Anti-Retaliation Law

Fear of retaliation is the most common reason people with valid whistleblower cases do not come forward. This fear is understandable — and it is also why Congress built robust anti-retaliation protections directly into the False Claims Act.

FCA Section 3730(h) — anti-retaliation protection

The FCA's anti-retaliation provision protects employees, contractors, and agents who engage in protected activity related to a qui tam case. Protected activity includes:

- Investigating potential FCA violations
- Filing or helping to file a qui tam lawsuit

- Testifying in an FCA proceeding
- Reporting fraud internally (in some circumstances)

If your employer fires, demotes, harasses, or otherwise discriminates against you because of this activity, you are entitled to reinstatement, double back pay, and reasonable attorneys' fees. These remedies exist on top of any relator share you may receive.

Security clearances

This is one of the most anxiety-inducing concerns for cybersecurity insiders. The practical answer, based on current law and practice, is that filing a qui tam lawsuit under seal does not inherently trigger a security clearance review, because the case is filed confidentially. If your clearance becomes an issue during litigation, your attorney will address it directly. The government has a strong interest in protecting whistleblowers who help it identify fraud — taking away their clearances would undermine that interest.

That said, if your employer learns you have filed and retaliates — including by challenging your clearance — you have legal remedies under the FCA's anti-retaliation provision and potentially under the Intelligence Community Whistleblower Protection Act or DoD whistleblower statutes depending on your specific situation.

NDA — are you bound by your non-disclosure agreement?

This is a question almost every cybersecurity whistleblower asks, and the answer surprises most people: NDAs generally cannot prevent you from filing an FCA qui tam case.

Courts have consistently held that private contracts cannot override federal law. An employer's NDA does not eliminate your right to file a qui tam lawsuit, cooperate with DOJ investigators, or testify in a government proceeding. NDAs can, however, affect what you can publicly disclose outside of the litigation process — another reason to work through counsel rather than acting unilaterally.

Can I file anonymously?

You can file a qui tam complaint through your attorney without your name appearing in public. The complaint is filed under seal, and your identity is not disclosed to the defendant or the public during the investigation period. If the case proceeds to trial or public settlement, your involvement may eventually become known — but in many cases, especially those that settle, relators maintain a significant degree of privacy.

Do not report internally before consulting an attorney

Many whistleblowers instinctively try to raise concerns internally first. In some industries, this is required by other laws — but in the cybersecurity fraud context, reporting internally before filing a qui tam case can alert the company to cover its tracks, result in immediate retaliation, and in some cases forfeit your status as an original-source relator. Consult an attorney before you say anything to your employer about your concerns.

Section 7: What Evidence You Need — and How to Preserve It Safely

You do not need a perfect evidentiary file to file a qui tam case. Whistleblower attorneys file complaints based on firsthand knowledge and limited documentation all the time — discovery, conducted after the complaint is filed, is how the full picture is assembled. That said, more specific and documented knowledge produces stronger cases and more leverage in settlement negotiations.

Types of evidence that support cybersecurity FCA claims

- SPRS score submissions and internal self-assessment documentation showing the real score vs. what was submitted to DoD
- System Security Plans (SSPs) that are clearly outdated, fabricated, or copied from templates without implementation
- Plan of Actions and Milestones (POA&M;) documents that show known deficiencies that were never remediated
- Internal audit reports, penetration test results, or vulnerability assessments showing non-compliance
- Emails or meeting notes from management acknowledging compliance gaps and instructing staff to certify anyway
- Incident reports that were prepared internally but never submitted to the government as required
- CMMC assessment documentation showing controls were falsely marked as implemented
- Contract clauses or certifications your company signed, coupled with internal documentation contradicting those certifications

What you should and should not do

DO	DO NOT
Write down what you know from memory — dates, conversations, specific incidents — while it is fresh	Access systems you are not authorized to use, even to document fraud
Preserve documents you received in the normal course of your job	Take documents in bulk, exfiltrate data, or copy systems you do not normally have access to
Note names of colleagues, supervisors, or executives who have knowledge	Tell colleagues you are considering a whistleblower claim
Keep a personal record of any retaliation, including dates and specifics	Report your concerns to your employer before speaking with an attorney

DO	DO NOT
Call an attorney before taking any further action	Wait — the first-to-file rule means delay has a real cost

The Computer Fraud and Abuse Act (CFAA) risk

The CFAA makes it a federal crime to access a computer system 'without authorization' or in excess of authorized access. If you access systems you are not permitted to use — even to gather evidence of fraud — you may expose yourself to criminal liability. The good news: evidence your attorney gathers through legal discovery is far more powerful than evidence you gathered in a way that could be challenged. Do not take this risk. Call first.

Section 8: Frequently Asked Questions

These are the questions we hear most often from cybersecurity professionals considering whether to come forward. They are answered in plain language, without unnecessary legal hedging — though every situation is different, and a consultation will give you answers specific to your facts.

What is the minimum SPRS score required by DoD, and what happens if a contractor falsifies it?

DoD does not set a minimum passing SPRS score — a contractor with any score can still hold a contract. The fraud occurs when a contractor submits an inflated score to make itself appear more compliant than it is. Because the SPRS score is a self-assessment, the gap between what was submitted and what an honest assessment would show is entirely internal knowledge — making insiders uniquely positioned to expose this fraud.

What is the difference between reporting cybersecurity fraud to CISA versus filing a qui tam lawsuit?

CISA (Cybersecurity and Infrastructure Security Agency) is a federal agency focused on improving national cybersecurity — it is not a law enforcement or fraud-recovery agency. Reporting to CISA may prompt guidance or advisories, but it does not result in financial recovery for the government or a relator share for you. An FCA qui tam lawsuit filed through the DOJ is the mechanism for financial accountability. The two are not mutually exclusive, but if you are considering a qui tam case, speak to an attorney before contacting any government agency.

Do I need to still be employed to file a qui tam case?

No. Former employees file successful qui tam cases regularly. The FCA's original-source requirement looks at whether you had direct and independent knowledge of the fraud — not whether you are currently employed. If you left the company because you raised concerns, or because the environment became untenable after you

flagged compliance issues, your departure may itself be evidence of retaliation.

What is 'materiality' in a cybersecurity FCA case, and why does it matter?

Materiality is the legal standard that asks: Would the government have paid the contractor if it had known the truth? After the Supreme Court's 2016 *Universal Health Services v. Escobar* decision, materiality became a contested element in FCA cases. In the cybersecurity context, the DOJ has argued — and courts have largely agreed — that cybersecurity compliance is material to DoD's payment decisions, particularly when the relevant contract clause explicitly conditions payment on compliance. The CCFI was designed in part to address materiality arguments by demonstrating the government's consistent enforcement posture.

Can I blow the whistle on a CMMC assessment that I believe was fraudulent?

Yes — and this is one of the most significant emerging areas for cybersecurity qui tam cases. If you are a C3PAO assessor who was pressured to certify a contractor you knew was non-compliant, an employee at a contractor whose CMMC assessment was fabricated, or a subcontractor who was represented as assessed when it was not, you may have a strong FCA claim. CMMC fraud is structurally similar to the cases the DOJ has already prosecuted — false certification to receive DoD contract payments — and the enforcement infrastructure is already in place.

Will reporting this affect my security clearance?

Filing a qui tam case under seal does not automatically trigger a security clearance review. The case is confidential from the outset. If your employer discovers your involvement and retaliates by challenging your clearance, you have legal remedies — and your attorney will address them directly. The government's interest in protecting whistleblowers who expose fraud is aligned with protecting your clearance, not threatening it.

What if the DOJ decides not to intervene in my case?

A declination is not a dismissal. The Whistleblower Advocates has specific experience litigating declined qui tam cases — a critical distinction, because many whistleblower firms do not have the resources or experience to proceed in declined cases. If the government declines, we evaluate the evidence, the damages, and the defendant's likely litigation strategy before advising whether to proceed. In declined cases, the relator share increases to 25–30%.

How long does a cybersecurity FCA case take?

Most cases take three to six years from filing to resolution, though some resolve faster through early settlement. The seal period alone typically runs one to three years. This is a long process — but it runs largely in the background of your life once the complaint is filed. Your attorney handles the DOJ investigation, court filings, and settlement negotiations. Your primary obligation after filing is availability for interviews and document review.

Can I file even if my company is also a cybersecurity company — not just a contractor?

Yes. The FCA applies to any entity that receives federal funds and makes false representations in connection with that funding. Cybersecurity firms, IT service providers, managed security service providers (MSSPs), and cloud vendors that hold federal contracts or are FedRAMP authorized are all potentially subject to the FCA.

Several of the most significant recent cybersecurity FCA cases have involved cybersecurity vendors themselves.

What if I only have partial information — I know something is wrong but don't have documents?

You do not need a complete documentary record to file. Oral testimony, specific recollections of conversations, and knowledge of what controls were and were not in place is meaningful evidence. The complaint is a starting point — discovery produces documents. What matters most at the outset is the specificity and credibility of your firsthand knowledge. An attorney can evaluate whether what you know is sufficient to file.

Is there a deadline to file?

The FCA has a six-year statute of limitations from the date the false claim was submitted, or three years from when the government knew or should have known about the fraud — whichever is later, and not to exceed ten years. However, the first-to-file rule means that a competitor or colleague filing first can cut off your right to recover. The relevant deadline is often: before someone else files. Do not treat the six-year statute as a reason to wait.

Do I have to testify publicly?

Most FCA cases settle before trial, and most relators never testify in open court. Your identity may be disclosed in connection with settlement documents or press releases, but many settlements are structured to minimize public identification of the relator. Your attorney will negotiate these terms. If the case does proceed to trial, your testimony would be required — but this is relatively uncommon.

What does it cost to hire The Whistleblower Advocates?

Nothing upfront. The Whistleblower Advocates works on a contingency basis — you pay no attorneys' fees unless we recover money for you. If the case succeeds, the defendant pays your attorneys' fees separately from your relator share under the FCA. The initial consultation is always free and confidential.

Section 9: Cybersecurity FCA Case Library

The following cases represent the growing body of cybersecurity False Claims Act enforcement. They are included to illustrate the range of conduct that has generated federal liability and the types of whistleblowers who have brought these cases forward. This library is updated as new cases are resolved.

Raytheon Companies / Nightwing Group — \$8.4 Million (2025)

Raytheon, later Nightwing Group, failed to implement required cybersecurity controls — including a System Security Plan — in a system used for unclassified DoD work. The failures covered the period 2015–2021. The case was brought by Branson Kenneth Fowler, a former Director of Engineering at Raytheon, under the FCA qui tam provisions. The settlement resolved violations of DFARS 252.204-7012 and FAR 52.204-21.

Aerojet Rocketdyne — \$9 Million (2023)

Defense contractor Aerojet Rocketdyne settled for \$9 million after a qui tam relator alleged the company falsely certified compliance with cybersecurity requirements in contracts with DoD and NASA. The case was one of the first major CCFI settlements and established the enforcement template for subsequent cybersecurity FCA cases.

Penn State University — \$1.25 Million (2024)

Penn State agreed to pay \$1.25 million to resolve allegations that it failed to implement required cybersecurity controls in its DoD research contracts, and failed to ensure subcontractor compliance with DFARS cybersecurity requirements. The case is significant for two reasons: it demonstrates that universities and research institutions face the same FCA exposure as defense primes, and it shows that failure to flow cybersecurity requirements down to subcontractors is itself actionable.

Insight Global — \$2.7 Million (2023)

Staffing and IT services firm Insight Global settled for \$2.7 million after allegations that it mishandled personally identifiable information in connection with a COVID-19 contact tracing contract. While not a DFARS cybersecurity case, it demonstrates that cybersecurity-adjacent failures — inadequate data protection under a government contract — generate FCA liability outside the defense sector.

Gen Digital (formerly Symantec) — \$55.1 Million (2024)

While this case centered on GSA contract pricing fraud rather than cybersecurity compliance fraud, it is notable as one of the largest settlements by a major cybersecurity firm, and illustrates the government's willingness to pursue significant recoveries against well-known vendors in the cybersecurity space.

Pattern recognition across these cases

In every case above: (1) there was an insider with direct knowledge of the gap between representation and reality; (2) the gap was documented, at least partially, in internal records; (3) the government recovered multiple times the amount of any single contract payment; and (4) the qui tam mechanism was the primary enforcement vehicle. These cases are not outliers — they are the template.

Ready to Take the Next Step?

If you have read this guide and believe you have knowledge of cybersecurity fraud against the U.S. government, the most important thing you can do right now is speak with an experienced whistleblower attorney — confidentially, at no cost, and with no obligation.

At The Whistleblower Advocates, we handle FCA cybersecurity cases exclusively on a contingency basis. You pay nothing unless we recover money for you. Our attorneys have specific experience with DFARS, CMMC, NIST 800-171, and SPRS compliance fraud, and with litigating both intervened and declined qui tam cases.

We can tell you within a single consultation whether your situation has the elements of a viable qui tam claim, what evidence you need, and what the process will look like for your specific facts. That conversation costs you nothing.

The Whistleblower Advocates

Free · Confidential · No Obligation

(833) 310-3147

thewhistbloweradvocates.com

Serving clients nationwide · Pennsylvania · New Jersey · Delaware · Georgia · and beyond

This guide is for general informational purposes only and does not constitute legal advice.

No attorney-client relationship is created by reading this material.

Copyright © The Whistleblower Advocates. All rights reserved.

This guide is for general informational purposes only and does not constitute legal advice. No attorney-client relationship is created by reading this material. Copyright © The Whistleblower Advocates. All rights reserved.