

# Federal Contracting

What tech companies need to know

# About Dentons' Silicon Valley Institute on Government and Technology

As part of our Silicon Valley Institute on Government and Technology, three leading practitioners in Dentons' Government Contracts Practice have prepared a thought piece that describes the handful of key contracting-related issues that technology companies should keep on their radar when doing business with the Federal Government. We look forward to the continuing discussion of these and other related issues at the intersection of the Government and Technology.

## About the Authors



Susan A. Mitchell has extensive experience in federal and California state litigation. Her primary practices are commercial litigation and representation of federal contractors in government investigations and enforcement proceedings. She advises clients on reporting under the Federal Acquisition Regulation (FAR) Mandatory Disclosure Rule, and compliance issues under the False Claims Act (FCA), the Anti-Kickback Act, the Foreign Corrupt Practices Act (FCPA) and other federal statutes and regulations. She has conducted more than 50 internal investigations, and successfully represented contractors in more than 20 investigations by the Department of Defense (DOD) Office of Inspector General, the National Aeronautics and Space Administration (NASA) Office of Inspector General, the Defense Criminal Investigative Service (DCIS), the Naval Criminal Investigative Service (NCIS) and the National Reconnaissance Office (NRO).



Kevin Lombardo focuses his practice in government contract law and international trade regulations. He has more than a decade of experience handling matters involving the following international trade regulations: International Traffic in Arms Regulations (ITAR); Export Administration Regulations (EAR); trade embargoes imposed by the Office of Foreign Assets Control (OFAC); FCPA; regulations enforced by the Committee on Foreign Investment in the United States (CFIUS); and the Anti-boycott Regulations.



J.W. Lafferty focuses his practice on government contract law and international trade regulations. J.W. handles federal government contracting issues, including contract formation, compliance, disputes, claims, terminations and allegations of fraud. In the international trade realm, J.W. handles matters involving ITAR, EAR, FCPA and OFAC issues, as well as supply chain management.

# Table of Contents

Introduction	4
1. Considerations when entering into Other Transaction Agreements (OTAs)	5
2. Flow-down clauses: Mandatory vs. non-mandatory	7
3. Cyber-security: Guarding the supply chain	8
4. Government supply chain management and sourcing obligations	10
5. Protecting your data rights	12
6. Internal compliance control systems	14
Conclusion	16



# Federal contracting: What tech companies need to know

By Susan Mitchell, Kevin J. Lombardo and J.W. Lafferty



When negotiating the terms and conditions of a technology contract with the US government (the Government), the predominant business issues are the parameters of performance, the period of performance and the terms of payment.

However, it is important to also give careful consideration to other proposed or non-negotiable contract requirements, some of which may be included in the contract only by reference, as they may increase or decrease your business risks, affect the scope of your compliance obligations or jeopardize the protection of your proprietary data.

This article details what a tech company needs to know before contracting with the Government,

how careful adherence to compliance obligations may actually increase your business efficiency, and how to reduce the downside risks of entering into a contract with the Government. We provide an overview of six areas that could ultimately affect your bottom line:

- Use of "Other Transaction" Agreements (OTAs)
- Flow-down clauses for subcontractors and suppliers
- Clauses imposing supplier sourcing obligations
- The DoD's updated cyber security rule
- Data rights clauses
- The Federal Acquisition Regulation's (FAR's) "Contractor Code of Business Ethics and Conduct" clause.



# 1. Considerations when entering into OTAs

OTAs are an essential component of the Government's plan to engage the technical innovator whose wish is to be a "nontraditional" government contractor.

OTAs are acquisition instruments designed specifically to facilitate "leading edge" R&D and prototype projects in a "relatively unstructured environment" with companies that are "unwilling or unable to comply with the government's procurement regulations." See generally the System of Systems Security Inc.'s (SOSSEC's) helpful website, <https://sossecconsortium.com/ota.cfm>. Variations of OTAs (or, in the case of R&D projects, "Technology Investment Agreements," or TIAs) are used by NASA, the DoD, the Department of Homeland Security, the Department of Energy and several other federal agencies.

There are many benefits to contracting with the Government through an OTA.

- Federal funding can be obligated more quickly than through a traditional contract vehicle, as OTAs are not subject to the FAR or Cost Accounting Standards (CAS), or to procurement statutes such as the Procurement Integrity Act, the Truth in Negotiations Act or the Competition in Contracting Act.
- While competition is required "to the extent practicable," an OTA award, unlike a typical government contract awarded under the FAR, cannot be protested at the Government Accountability Office (GAO).
- Unlike traditional government procurements, the Government is allowed to openly discuss requirements and collaborate with contractors to determine the best approach for achieving the deliverable product.
- OTAs are not automatically subject to a Defense Contract Audit Agency (DCAA) audit, although in most circumstances the Government likely will seek to include specified audit rights in the OTA.
- Government rights to intellectual property are far more negotiable than for traditional government contracts.

But there are some potential drawbacks to such agreements.

- The Code of Federal Regulations (CFR) encourages Agreements Officers to negotiate rights “necessary to accomplish program objectives and foster Government interests,” which typically entails securing, at a minimum, “government purpose” rights in the deliverable, where some government funding has been used for development.
- OTAs generally are awarded on a firm-fixed-price basis and payments typically are based on measurable milestone achievements—criteria that can be risky in a developmental environment. Before a contractor enters into an OTA, the contractor should carefully assesses the technical risks, prospective costs and the feasibility of the

Government’s proposed milestones.

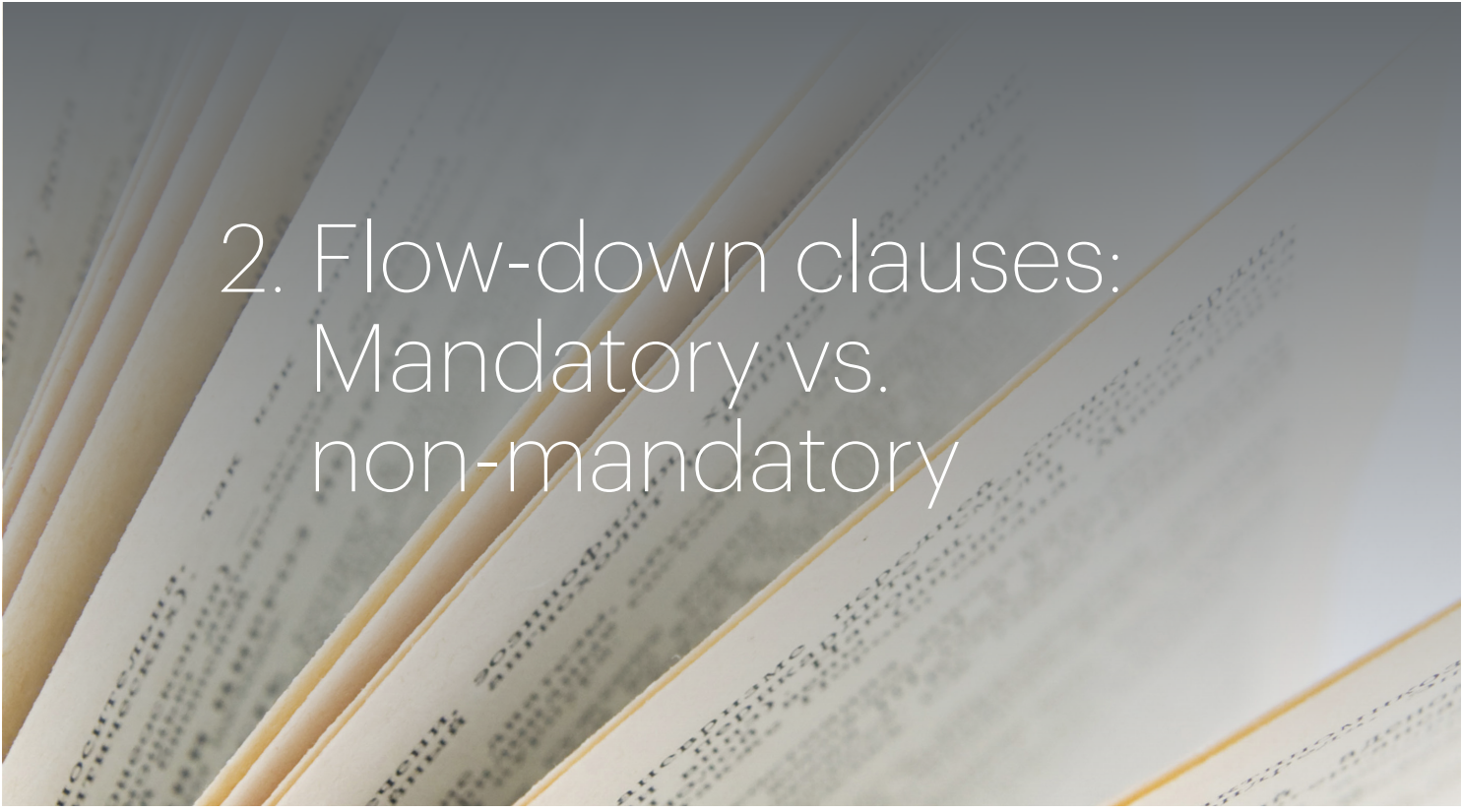
- While OTAs offer far fewer statutory and regulatory constraints on the conduct of the contractor’s program than do regular contracts, there are still constraints and it is critically important to understand what they are. Traditional commercial technology companies contemplating an OTA should, for example, familiarize themselves with the Government’s proposed terms and conditions for foreign access and domestic manufacturing requirements, and required systems for limiting or accounting for incurred costs, as well as some of the Government’s socio-economic principles that might be applicable, such as Executive Order 11246 (regarding Equal Employment Opportunity) and the Service Contract Act, 41

U.S.C. §351 et seq.

- One should also bear in mind that OTAs, while significantly streamlined in their requirements, may still contain or be subject to government remedies for fraud, such as suspension/debarment clauses, or potential liability under the civil False Claims Act, 31 U.S.C. §3729 et seq.







## 2. Flow-down clauses: Mandatory vs. non-mandatory

Government contracts typically are littered with obligations, some in contract-specific clauses and others in clauses incorporated by reference. When negotiating subcontracts, it is important for both the prime contractor and the subcontractor to know the differences between flow-down clauses mandated by the FAR or the DoD's Defense FAR Supplement (DFARS), and clauses that a Government customer may include in the prime contract that need not be flowed down to subcontractors.

Mandatory flow-down clauses vary by contract type, contract value and/or other extrinsic statutory/regulatory requirements. Even contracts for commercial items have mandatory flow-down clauses—14 at current count. Many of these clauses are characterized by the Government as socio-economic in nature. They include, for example, the "Equal Opportunity" clause, FAR 52.222-26; the "Notification of Employee Rights Under the National Labor Relations Act" clause, FAR 52-222-40; the

"Combat Trafficking in Persons" clause, FAR 52.222-50 (which implements Executive Order 13627, "Strengthening Protections Against Trafficking in Persons in Federal Contracts"); and the "Encouraging Contractor Policies to Ban Text Messaging While Driving" clause, FAR 52.223-18, all of which must be flowed down to subcontractors, even if the clauses seem irrelevant to subcontract performance.

Other clauses are not mandatory flow-downs, but may be useful, or

essential, to protect the prime. For example, FAR 52.249-1, "Termination for Convenience of the Government," is not a mandatory flow-down clause, but if you are the prime contractor and your contract is terminated at a moment's notice by the Government, you would be wise to have included a similar clause in your subcontracts, so you do not remain obligated to subcontractors, other than with respect to the obligations that survive a termination for convenience by the Government.

A person in a plaid shirt is standing in a server room, looking at a rack of servers. The room is dimly lit with blue light emanating from the server racks. The text "3. Cyber security: Guarding the supply chain" is overlaid in white.

### 3. Cyber security: Guarding the supply chain

Recognizing the potentially catastrophic consequences of security breaches of federal databanks and IT systems, the Government updated FAR 52.204-21 (2016), “Basic Safeguarding of Covered Contractor Information Systems,” and DFARS 252.204-7012 (2013), now called “Safeguarding Covered Defense Information and Cyber Incident Reporting.” See 81 Fed. Reg. 30439, 30446 (May 16, 2016).

The new rule, issued by the DoD, the GSA and NASA, requires prime contractors to “rapidly report” cyber incidents to DoD at a specified website, and to “conduct a review [of covered defense information] for evidence of compromise,” including identifying compromised computers, servers and data, and “analyzing” the associated information systems. Upon request by the Government, contractors who suffer a cyber incident “shall” provide the DoD with access to additional information or equipment that is “necessary to conduct a forensic analysis.”

If you are a large tech company, you likely already have a robust cyber security system consistent with the Government’s requirements. Most hackers these days, however, do not target billion-dollar enterprises directly; they target the enterprises’ more vulnerable supply chains. The new rule therefore makes the revised DFARS 252.204-7012 a mandatory flow-down clause to subcontracts and “similar contractual instruments” that involve a covered contractor information system or that provide “operationally critical support.” The designation of “operationally critical”

goods or services will be made by the Government. The new rule also requires the prime to include a provision in the subcontract requiring the sub to rapidly report cyber incidents not only to the prime, but directly to the Government.

These new requirements raise issues as to the appropriate level of prime contractor oversight of subcontractor security systems; depending on the sophistication of the subcontractor and the type of covered information the subcontractor is protecting, a certification from the subcontractor



that it is compliant with the security requirements of the new rule, including implementation of the framework for critical infrastructure set forth in the National Institute of Standards and Technology's Special Publication No. 800-171 (NIST 800-171), may or may not suffice as adequate due diligence. As a practical matter, depending again on your assessment of the risk of breach and the potential consequences of a breach, you may consider negotiating with the subcontractor for an indemnity clause or even insurance coverage.

Note: Covered contractors are required to implement NIST 800-171 controls "as soon as practicable," but no later than December 31, 2017.

"If you are a large tech company, you likely already have a robust cyber security system consistent with the Government's requirements. Most hackers these days, however, do not target billion-dollar enterprises directly; they target the enterprises' more vulnerable supply chains."





## 4. Government supply chain management and sourcing obligations

Government statutes and regulations affect how you build your product, charge your costs and conduct your program. One element of most contracts that may be overlooked during contract negotiations are the sourcing obligations and restrictions prescribed by the Buy American Act (BAA), the evolving DFARS rule for the detection and avoidance of counterfeit electronic parts, and the Combat Human Trafficking in Persons clause. Each of these clauses is a potential compliance risk; and because the subject matter of each has a high public profile, noncompliance poses a significant litigation risk.

The BAA requires the Government to prefer U.S.-made products in certain qualifying purchases. See 41 U.S.C. § 8301 et seq. The BAA restricts the delivery of foreign end products under federal government contracts by granting a price preference advantage to contractors proposing competing offers of domestic end products. It

applies to supply and construction contracts between \$3,000 and the dollar threshold for Trade Agreements Act applicability (currently \$191,000 for a supply contract and \$7,358,000 for a construction contract). It also applies to certain procurements without regard to their value, including purchases of arms, ammunition or

war materials; indispensable national security purchases; sole-source acquisitions; and small business set-aside contracts.

Under a new Counterfeit Parts regulation, "Detection and Avoidance of Counterfeit Electronic Parts," proposed September 21, 2015, DoD



contractors would be required, with limited exceptions, to obtain electronic parts only from “trusted suppliers” as part of their mandatory detection and avoidance system for counterfeit electronic parts. 80 Fed. Reg. 56939. The proposed rule clarifies the existing requirement that DoD contractors must be able to trace their supply chain of electronic parts back to the original manufacturer by establishing “risk-based” traceability. The required system must take into consideration the probability of receiving a counterfeit electronic part; the probability that inspection or testing will detect a counterfeit; and the potential negative consequences of installing a counterfeit part in the deliverable item. The proposed rule further requires that if a contractor cannot establish traceability from the original manufacturer for a specific part, the contractor must complete an evaluation that considers alternative parts, or testing and inspections commensurate with the assessed risk of the suspect part being counterfeit. After considering comments from the contracting community on the original draft of the rule, the DoD narrowed the rule’s definition of “electronic part” by removing the categories of “embedded software or firmware.”

More recently, a revision to DFARS 231.205-71 that was proposed on March 25, 2016, would disallow all costs associated with suspect counterfeit parts, including rework and corrective action, unless the contractor (i) has a DoD-approved system to detect suspect parts, (ii) followed sourcing regulations, and (iii) timely reported the problem. 81 Fed. Reg. 17055.

Recent regulatory changes to FAR and DFARS Human Trafficking clauses pose another source of supply chain management compliance risk. In January 2015 the FAR was amended to impose greater responsibilities on prime contractors and subcontractors to train and monitor compliance by their respective employees and “agents.” See 80 Fed. Reg. 4967, Ending Trafficking in Persons (codified in several sections of the FAR and DFARS). The substance of the clause at FAR 52.222-50 must be flowed down to “all subcontracts” and “all contracts with agents,” regardless of contract price or location of performance. Prime contractors are required to be “vigilant” in monitoring subcontractors and employees, and contractors must report “credible information” about human trafficking violations to the

Contracting Officer and the procuring agency’s OIG. In addition, for contracts and subcontracts as to which more than \$500,000 in services or supplies are to be performed outside of the United States (other than commercial off-the-shelf (COTS) items), the revised federal rules impose obligations to implement and monitor compliance plans and provide annual certifications, among other requirements.

Given the high visibility of this issue in the national press, compliance with Human Trafficking prohibitions and requirements is unlikely to be a problem at a prime contractor’s own facility. However, the prime’s obligation to police subcontractor and agent compliance can be difficult, particularly if the item at issue is produced in a third-world country. Your best protection is a robust compliance oversight system, designed and implemented with careful attention to the nuances of the FAR and DFARS clauses, and well-trained employees, subcontractors and agents.





## 5. Protecting your data rights

A significant issue for tech companies that are negotiating government contracts for non-commercial items is how best to protect intellectual property. Issues to consider carefully are the particular data rights clauses the Government is proposing to include in the contract or OTA; the extent to which government funds will be used to develop the technical data used in contract performance; how your company is going to ensure that technical data and other proprietary information is marked with FAR-approved legends; and how your company is going to maintain traceability of the time and expenses incurred in developing the data at “private expense.”

Under the FAR, the contractor retains ownership of a delivered item’s intellectual property, and the Government contractually acquires a license in that data. The FAR and DFARS provide for three types of licenses in “technical data,” defined as recorded information of a scientific or

technical nature, including databases and software documentation:

1. “Limited rights,” a license that precludes the Government from releasing the technical data “outside the Government” absent exigent circumstances;
2. “Government purpose rights,” a license that allows the Government, among other things, to “[u]se, modify, reproduce, . . . or disclose technical data within the Government without restriction,” and to authorize persons “outside the Government”

to use or modify the technical data “for United States government purposes,” including competitive procurements; and

3. “Unlimited rights.” See generally DFARS 252.227-7013.

The FAR and DFARS also provide analogous government licenses for “computer software,” defined in the FAR as including programs, source code, algorithms and related data that would enable the software to be reproduced or recompiled.

To qualify for limited rights status:

1. The technical data must be “developed at private expense,” meaning development of the data was not required (e.g., funded) under a government contract, and the data is a trade secret or confidential information of the company;
2. The development costs must be charged to an indirect cost pool; and
3. The documentation of the technical data must be marked with an “appropriate legend” (i.e., one of the legends set forth in the FAR and DFARS). See, for example, FAR 2.101, 27.401, 27.404-2(b), 52.227-14(g)(3)(Alt. II).

A key issue for companies that plan to expand or modify their existing technology through government funding is determining whether, and at what point, the Government obtains rights in the technology. Under the FAR and DFARS, technical data is “developed” when it is “workable.” See generally DFARS 252.227-7013(a)(7), “Rights in Technical Data — Noncommercial Items.” Long-established case law holds that workability is established when the item has been analyzed or tested sufficiently “to demonstrate to reasonable people skilled in the applicable art that there is a high

probability that it will operate as intended.” For example, the Ninth Circuit found that a device had been “developed” prior to contract award because the device at the point of contract award had a “high probability of success.” The court held that subsequent government funding to improve the device’s performance did not constitute “development.” See *Dowty Decoto, Inc. v. Dept. of the Navy*, 883 F.2d 774, 780 (9th Cir. 1989). The status of technical data as “developed,” in whole or in part, is often the subject—or should be the subject—of a focused discussion between the contractor and the government customer during contract negotiations.

The status of technical data as “developed,” in whole or in part, is often the subject—or should be the subject—of a focused discussion between the contractor and the government customer during contract negotiations.

Note that protecting limited rights or government purpose rights in technical data depends on the adequacy and consistency of the contractor’s documentation throughout contract performance. Mere imposition of a legend on or

in technical data will not, without more, suffice to protect that data; the contractor must also have documentation sufficient to demonstrate that the technical data was developed and charged in accordance with the FAR’s criteria. This is not to detract from the importance of the legend: Even if data was developed exclusively at private expense and the contractor has documented those costs appropriately, the contractor will have limited rights in the data only if the data is marked with the “appropriate” legend. See generally 10 U.S.C. §2321; DFARS 252.227-7037(b)-(c).

Moreover, data not properly marked with the appropriate legend can be subject to a Freedom of Information Act request (i.e., the Government may be legally required to disclose your proprietary data to any member of the public—including your competitor—who requests it, if the data is not properly marked and traceability documentation is not maintained during and after contract performance.) It is therefore critically important to have at the outset of performance a set of specific procedures in place, and periodic employee training, to ensure that amidst the creative process essential to leading edge or beyond-state-of-the-art projects, there is also rigorous discipline in both cost traceability and rights documentation.





## 6. Internal compliance control systems

FAR 52.203-13, “Contractor Code of Business Ethics and Conduct” applies to DoD contracts that have a contract value, including unexercised options, of more than \$5 million and a period of performance longer than 120 days.

### **There are three important requirements in FAR 52.203-13:**

First, the clause requires the contractor to maintain an internal control system that, among other specified criteria, must assign compliance responsibilities “at a sufficiently high level and [with] adequate resources to ensure effectiveness” of the internal controls. The internal control system must be monitored and audited, and the controls system must provide an internal reporting mechanism that encourages employees to report, confidentially or anonymously, “suspected instances of improper conduct.”

Second, the clause is a mandatory flow-down clause for subcontracts and sub-tier suppliers that fall within the clause’s coverage threshold.

Third, the clause includes a requirement for mandatory disclosure by the contractor to the Contracting Officer and the DoD Office of Inspector General (OIG), when the contractor has “credible evidence” (an undefined term) that a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act (FCA) or a violation of federal criminal law under Title 18 of the US Code involving fraud, conflicts of interest, bribery or illegal

gratuities; or that there have been “significant” overpayments (another undefined term) to the contractor by the Government. Further, failure to “timely” (yet another undefined term) disclose such evidence may expose the contractor or subcontractor to suspension or debarment under FAR 9.406 or 9.407. The National Reconnaissance Office (NRO) has an even broader mandatory disclosure rule.

By far the most frequent subject of mandatory disclosures are potential violations of the FCA. A contractor’s decision to make, or not make, a disclosure to the DoD’s OIG should be



made with the advice of experienced counsel. The FCA is replete with vague liability criteria. It proscribes any “false” claim for payment, or false statement in support of a claim for payment, made intentionally or “recklessly,” that is “material” to a contracting officer’s decision to pay the claim. “Reckless” conduct and “materiality” often are in the eye of the beholder; FCA “recklessness” is defined (unhelpfully) in case law as misconduct beyond gross negligence; and the “materiality” of a “false” statement or claim is defined by statute (expansively) as having “a natural tendency to influence” the contracting officer’s payment decision.

The U.S. Supreme Court recently confirmed the prior rulings of a number of courts of appeal that FCA “falsity” can include falsity “implied by law.” See *Universal Health Services, Inc. v. United States ex rel. Escobar*, 579 U.S. \_\_\_, 2016 WL 3317565 (June 16, 2016). This “implied certification” doctrine imposes FCA liability for

an intentional or reckless violation of any requirement of contract, statute or regulation, where the contractor makes specific representations to the Government about the goods or services provided, but the contractor’s failure to disclose its noncompliance with a “material” requirement “makes those representations misleading half-truths.” While the Court’s decision means that contractors will continue to be subject to FCA liability even where they have not made an express false representation, the Court emphasized that “materiality” is a “demanding” standard that cannot be met by “minor or insubstantial” noncompliances.

Most defense contractors are generally aware of the FCA, but many contractors view the statute as a low risk for honest companies. Not so. The FCA permits whistleblowers (called “qui tam relators”) to file an FCA action on the Government’s behalf in return for up to 30% of the treble damages mandated by the statute, or any proceeds from settlement, plus

reasonable expenses and attorney’s fees. Qui tam relators—often current or former employees—range from the brave and truthful whistleblowers contemplated by the FCA, to “true believers” who erroneously interpret contract specifications or incorrectly view minor noncompliant acts or omissions as fraud, to outright opportunists who hope that a contractor facing expensive litigation will opt for settlement.

In FY 2015, 737 FCA cases were filed, 632 of them by whistleblowers. The Government almost never moves to dismiss a qui tam action, even when it has decided not to intervene and prosecute the claims itself.

The best way to reduce your risk of getting sued under the FCA is to maintain a FAR-compliant internal controls system, conduct thorough and effective employee and manager training, and take prompt action to investigate employee complaints of misconduct.



# Conclusion

While contracting with the government may open new funding vistas and revenue streams, it also carries unique legal and business risks. Paying careful attention to the terms of your agreement, seeking legal counsel on issues that are complex or risky, and implementing and auditing robust compliance systems should mitigate most performance risks and ensure that your venture into the world of government contracting is successful and profitable.

