



# Doing Business with the Federal Government: Understanding the Unique Risks Associated with Government Contracts

**Lori Ann Lange**

Partner

Co-chair, Government Contracting & Infrastructure  
Washington, DC Office

NEW YORK, NY • RIVER EDGE, NJ • MIAMI, FL • WASHINGTON, D.C. • LOS ANGELES, CA • OAKLAND, CA  
CHICAGO, IL • AUSTIN, TX • DALLAS, TX • HOUSTON, TX • [WWW.PECKLAW.COM](http://WWW.PECKLAW.COM)

# WHAT IS A GOVERNMENT CONTRACT?

- Contract directly between the Federal Government and a contractor
- Different from contracts where the Federal Government is not a party but provided some form of assistance (*e.g.*, grant, loan, mortgage insurance, etc.)
- Different from contracts with state and local governments, although some concepts are the same

# GOVERNMENT CONTRACTS VS. COMMERCIAL CONTRACTS

- Highly regulated
- Terms are spelled out in the FAR clauses and the FAR agency supplement clauses
- Non-negotiable
- Limited or no discussions
- Government has significant discretion in administering the contract
- No contractor right to terminate the contract
- Numerous reporting requirements

# HOW TO BECOME A CONTRACTOR

- Identify which government agencies purchase your goods and services
  - Attend agency days
  - Search award data in [beta.SAM.gov](https://beta.sam.gov)
  - Search spending data in [usaspending.gov](https://usaspending.gov)
  - Check the GSA supply schedules
  - Talk with the agencies
- Register in the System for Award Management
- Complete the certs and reps
- Search for solicitations in [beta.SAM.gov](https://beta.sam.gov)

# KEY PLAYERS

- Contracting Officer (CO or KO)
  - CO is the person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings (FAR 2.101)
  - Authority may be limited to specified dollar amounts known as warrants
  - Can be different types of COs
    - Procurement Contracting Officer (PCO)
    - Administrative Contracting Officer (ACO)
    - Termination Contracting Officer (TCO)
- Contracting Officer's Representative (COR) and Contracting Officer's Technical Representative (COTR)
  - COR is the person, including a COTR, designated and authorized in writing by the CO to perform specific technical or administrative functions (FAR 2.101)

# AUTHORITY OF GOVERNMENT AGENTS

- Government is bound by the actions of its agents only when the agent is acting within the scope of his/her actual authority
- Apparent authority doctrine does not apply
  - “[A]nyone entering into an arrangement with the Government takes the risk of having accurately ascertained that he who purports to act for the Government stays within the bounds of his authority.”  
*Federal Crop Ins. Corp. v. Merrill*, 332 U.S. 380, 383 (1947)
- Contractors may be able to recover under the doctrines of implied authority and ratification

# AUTHORITY OF COS, CORS, AND COTRS

- In general, only the CO can:
  - Award contracts
  - Issue contract modifications
  - Make changes to the scope of work
  - Obligate the Government to pay money
- COR/COTR's role is generally limited to performing technical and administrative functions
- Government often will provide the contractor with notice of the scope of the COR's/COTR's authority
  - In the contract or in the award letter

# EXAMPLES OF LIMITATIONS ON AUTHORITY

- DFARS 252.201-7000, Contracting Officer's Representative

(b) If the Contracting Officer designates a contracting officer's representative (COR), the Contractor will receive a copy of the written designation. It will specify the extent of the COR's authority to act on behalf of the contracting officer. The COR is not authorized to make any commitments or changes that will affect price, quality, quantity, delivery, or any other term or condition of the contract.



# KEY RISKS – CERTIFIED COST OR PRICING DATA

- FAR 52.215-10, Price Reduction for Defective Certified Cost or Pricing Data; FAR 52.215-11, Price Reduction for Defective Certified Cost or Pricing Data - Modifications
- Contractor may be required to submit certified cost or pricing data with its proposal or with a change order proposal
- Cost or pricing data are all facts that reasonably can be expected to contribute to the soundness of estimates of future costs and to the validity of determinations of costs already incurred (FAR 2.101)
- Verifiable factual information – not subjective judgments
- More than just historical accounting data
- Includes data forming the basis for the contractor's judgment about estimated future costs or projections

# KEY RISKS – CERTIFIED COST OR PRICING DATA

- Certified cost or pricing data are required for:
  - Award of a negotiated contract over the cost or pricing data threshold
    - \$750,000 for prime contracts awarded before July 1, 2018
    - \$2M for prime contracts awarded on or after July 1, 2018
  - Award of a subcontract over the threshold at any tier if the contractor and each higher-tier subcontractor were required to submit certified cost or pricing data
  - Contract modifications exceeding the threshold regardless of whether certified cost or pricing data initially were required
    - Applies to modifications of fixed-price contracts

# KEY RISKS – CERTIFIED COST OR PRICING DATA

- Exceptions to the requirement to submit certified cost or pricing data are:
  - Adequate competition
    - Two or more offerors independently submit reasonably priced offers
    - For agencies other than the DoD, NASA, and the Coast Guard, one offer but there was a reasonable expectation that two or more offerors competing independently would submit offers and the offeror did not know it did not have competition
  - Prices set by law or regulation
  - Acquisition of commercial items
  - Agency waiver

## KEY RISKS – CERTIFIED COST OR PRICING DATA

- Contractor has to certify that the cost or pricing data submitted are current, accurate, and complete as of the date of final agreement on price
  - Current – data are up to date; disclosed the most up to date information
    - There is a continuing duty to update until an agreement on price is reached
  - Accurate – data disclosed are correct; no errors
  - Complete – all data required to be disclosed have been disclosed; no omissions

## KEY RISKS – CERTIFIED COST OR PRICING DATA

- FAR 52.215-10, Price Reduction for Defective Certified Cost or Pricing Data; FAR 52.215-11, Price Reduction for Defective Certified Cost or Pricing Data - Modifications
- Government is entitled to a price reduction for defective cost or pricing data if the contract price was increased by a significant amount
- Amount of the reduction is the amount by which the price was increased
  - Rebuttable presumption that this is dollar for dollar

# CLE CODE #1

PA1000

# KEY RISKS – COST PRINCIPLES

- FAR Subpart 31.2
- 46 Cost Principles that limit the recovery of various types of costs including:
  - Bonding costs
  - Compensation costs
  - Depreciation costs
  - Material costs
  - Rental costs
  - Travel costs
- Typical performance costs (*e.g.*, labor and materials) generally are allowable as long as the costs are reasonable

# KEY RISKS – COST PRINCIPLES

- Certain types of costs are unallowable:
  - Public relations and advertising costs
  - Bad debt collection
  - Alcohol and entertainment
  - Fines, penalties, and mischarging costs
  - Interest and other financial costs
  - Lobbying and political activity costs
- Certain types of cost are allowable under certain circumstances
  - Executive compensation
  - Idle facilities
  - Meals and lodging



## KEY RISKS – COST PRINCIPLES

- Used for the determination, negotiation, and allowance of costs
- Applicable to pricing of cost-reimbursement contracts
- Not applicable to the pricing of competitively bid fixed-price contracts unless cost analysis is performed
- Applicable to the pricing of modifications to both fixed-price and cost-reimbursement contracts

## KEY RISKS – COST PRINCIPLES

- When applicable, the Cost Principles require that costs charged to the Government be:
  - Allowable
  - Allocable
  - Reasonable

# KEY RISKS – GOVERNMENT AUDIT RIGHTS

- FAR 52.214-26, Audit and Records – Sealed Bidding; FAR 52.215-2, Audit and Records – Negotiation
- Government has the right to audit the contractor's books and records for contracts that are:
  - Cost-reimbursement
  - Incentive (*i.e.*, contracts where the contractor can earn an award fee or additional profit for reduced costs or improved delivery or technical performance)
  - Time-and-material
  - Labor-hour
  - Price-redeterminable (*i.e.*, contracts where the price is determined after an initial period of performance or after completion)

## KEY RISKS – GOVERNMENT AUDIT RIGHTS

- Government generally does not have the right to audit fixed-price contracts if certified cost or pricing data were not required
- Government can audit change orders under fixed-price contracts

# KEY RISKS – PREVAILING WAGES

- FAR 52.222-6, Construction Wage Rate Requirements; FAR 52.222-41, Service Contract Labor Standards
- Applicable to service and construction contracts
  - Contractors must pay their workers the applicable prevailing wage rate and fringe benefits set forth in the wage determination(s) contained in the contract
- Contractors must pay their workers overtime for any hours worked in excess of 40 hours/week
- Prime contractors are financially liable for subcontractor underpayments
- Failure to pay prevailing wage can result in contract termination as well as suspension and debarment

## KEY RISKS – FEDERAL MINIMUM WAGE

- FAR 52.222-55, Minimum Wages Under Executive Order 13658
- Contractors have to pay workers performing on, or in connection, with the contract at least the federal minimum wage of \$10.95/hour (2021 rate)
  - Not limited to laborers and mechanics
  - Includes apprentices
  - Applies to workers subject to the Fair Labor Standards Act (onsite receptionist, secretary/assistant, file/document clerk, etc.)
  - Fringes do not count toward the \$10.95/hour
  - Rate should go up in 2022

## KEY RISKS – PAID SICK LEAVE

- FAR 52.222-62, Paid Sick Leave Under Executive Order 13706
- Contractors have to give employees working on or in connection with the subcontract at least 1 hour of paid sick leave for every 30 hours worked up to 56 hours per year
- Paid sick leave is in addition to any fringe benefits required to be paid under the applicable prevailing wage laws

## KEY RISKS – BUY AMERICAN ACT

- FAR 52.225-1, Buy American – Supplies; FAR 52.225-9, Buy American – Construction Materials
- Contractors supplying end products or construction material have to comply with the Buy American Act (BAA)
- BAA is different from the Buy America requirements
- Buy America refers to the group of domestic content restrictions that are attached to funds administered by the U.S. DOT to make grants to states, localities, and other non-federal government entities for various transportation projects
  - There are different Buy America requirements within U.S. DOT itself
  - FTA, FHWA, FAA, or FRA have different Buy American statutes and regulations



## KEY RISKS – BUY AMERICAN

- Recent changes to the BAA FAR regulations
- On January 19, 2021, the FAR Council issued its final rule effective February 22, 2021
- Created a new category of end products/construction material – predominantly iron or steel end products/construction material
  - Must have less than 5% foreign iron or steel or both
- Increased the domestic content requirement for not predominantly iron or steel end products/construction materials from 50% to 55%

## KEY RISKS – BUY AMERICAN

- On January 25, 2021, President Biden issued an Executive Order regarding the BAA
- The Executive Order directs the FAR Council to consider revising the BAA FAR regulations to:
  - Replace the component test with a test under which domestic content is measured by the value that is added to the product through U.S.-based production or U.S. job-supporting economic activity;
  - Increase the numerical threshold for domestic content requirements for end products and construction materials; and
  - Increase the price preferences for domestic end products and domestic construction materials

## KEY RISKS – BUY AMERICAN

- BAA requirements can have a significant impact on price
- Post award waivers can be difficult to obtain and require the contractor to give consideration
- Noncompliance can result in a direction to rip it out and replace it

# CLE CODE #2

PA2500

## KEY RISKS – CHINESE TELECOM

- FAR 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment; FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
- Expands the previous ban on supplying certain Chinese telecom to the Government
- Requires the contractor to represent whether it uses certain covered Chinese telecom in its own internal operations

# KEY RISKS – CHINESE TELECOM

- Ban includes:
  - Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, including its subsidiaries or affiliates;
  - Video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, including its subsidiaries or affiliates;
  - Telecommunications or video surveillance services provided by such entities or using such equipment; or
  - Telecommunications or video surveillance equipment or services produced or provided by an entity reasonably believed to be an entity owned or controlled by, or otherwise connected to the Chinese government, as determined by the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation

## KEY RISKS – CHINESE TELECOM

- Contractors have to represent whether they use covered telecommunications equipment or services in their internal operations
- Contractors have to make a reasonable inquiry before making the representation
- Reasonable inquiry is designed to uncover any information in the contractor's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity
  - Reasonable inquiry does not necessarily require an internal or third-party audit

## KEY RISKS – CYBERSECURITY

- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- Defense contractors who will have access to Covered Defense Information (CDI) must take steps to implement the 110 security controls in NIST SP 800-171
- If the contractor is not in full compliance, it must have:
  - A System Security Plan (SSP) in place that details its plan for ensuring the security of CDI
  - A Plan of Action and Milestones (POA&M) that identifies the tasks that the contractor still needs to accomplish, the resources required to accomplish the plan, any milestones in meeting the tasks, and the scheduled completion dates for those milestones



## KEY RISKS – CYBERSECURITY

- DFARS 252.204-7021, Contractor Compliance with Cybersecurity Maturity Model Certification level requirement
- DFARS 252.204-7021 requires contractors to:
  - Be certified to at least the specified CMMC certification level prior to contract award
  - Maintain the required certification level for the duration of the contract
  - Ensure that subcontractors have the “appropriate” CMMC level prior to subcontract award
  - Flow the clause down to subcontractors

# KEY RISKS – CYBERSECURITY

## Levels

Level 1 (Basic Cyber Hygiene) – 17 practices

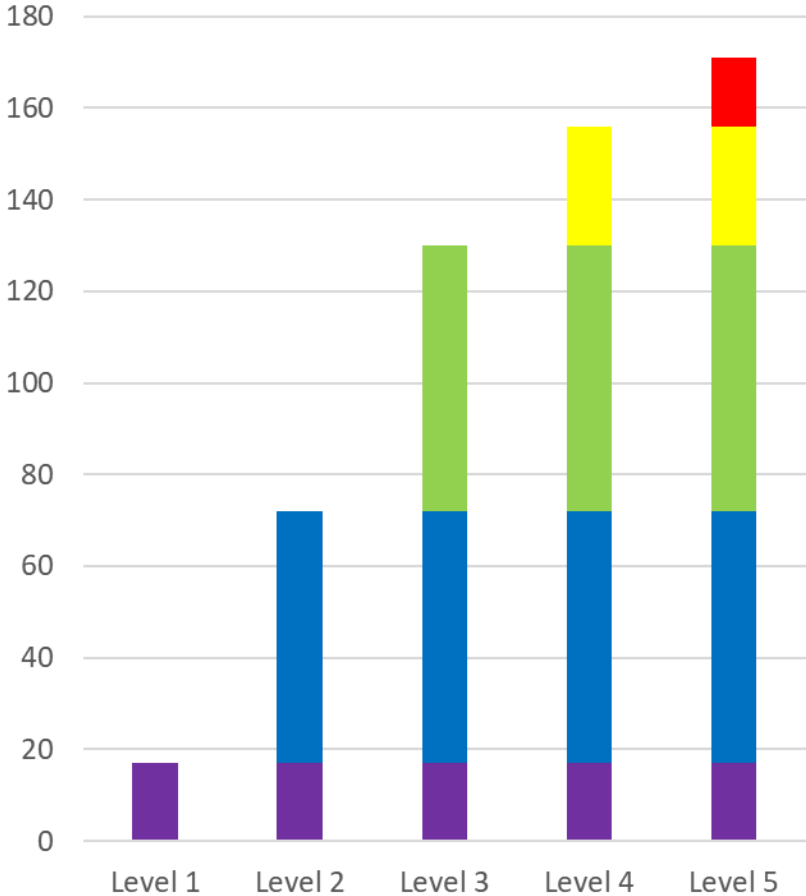
Level 2 (Intermediate Cyber Hygiene) – 72 practices in total (Level 1 practices + 55 additional practices)

Level 3 (Good Cyber Hygiene) – 130 practices in total (Levels 1-2 practices + 58 additional practices)

Level 4 (Proactive) – 156 practices in total (Levels 1-3 practices + 26 additional practices)

Level 5 (Advanced/Progressive) – 171 practices in total (Levels 1-4 practices + 15 practices)

## CMMC Practices



## KEY RISKS - CYBERSECURITY

- Until September 30, 2025, defense contractors only will need to be CMMC certified if the solicitation and contract require certification
- Starting on or after October 1, 2025, all defense contractors will need to be CMMC certified as a condition of contract award except for those selling commercially available off-the-shelf (COTS) items
- CMMC is being rolled out in phases and DoD has indicated that it expects to have up to 15 CMMC pilot contracts by the end of 2021

# KEY RISKS - CYBERSECURITY

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements; DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
- Contractors have to perform an assessment of their compliance with the NIST SP 800-171 security controls before the award of a new contract or the exercise of an option or contract extension when the contractor is required to implement NIST SP 800-171 under DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- Contracting Officers are required to verify that the contractor has a current (not older than three years) assessment on record prior to award

# KEY RISKS – CYBERSECURITY

- Three assessment levels – Basic, Medium, and High
- Basic – contractor’s self-assessment of its implementation of the 110 NIST SP 800-171 controls
- Medium – DoD review of the contractor’s Basic Assessment, a “thorough document review”, and discussion with the contractor to obtain additional information or clarification
- High – Medium Assessment with the addition of verification, examination, and demonstration of the contractor’s SSP to validate that the NIST SP 800-171 controls have been implemented as described in the SSP

## KEY RISKS – FALSE CLAIMS ACT

- Contractors performing government contracts are subject to the False Claims Act (FCA)
- There are two FCAs
  - Criminal statute – 18 U.S.C. § 287
  - Civil statute – 31 U.S.C. §§ 3729, *et seq.*

# KEY RISKS – FALSE CLAIMS ACT

- FCA prohibits (among other things):
  - Knowing submission of a false or fraudulent claim for payment or approval
  - Use of a false record or statement in a claim
  - A conspiracy to commit a violation of the Act
  - Failure to remit an overpayment (aka reverse false claim)

# KEY RISKS – FALSE CLAIMS ACT

- Elements of a false claim:
  - Submission of a claim for payment or approval
    - Term "claim" is defined broadly
    - Includes progress payment applications, certified payrolls, etc.
  - Claim was false or fraudulent
  - Contractor knew that the claim was false or fraudulent
  - Falsity was material
    - Can influence the decision to pay or approve the claim



# KEY RISKS – FALSE CLAIMS ACT

- Who can bring an FCA action?
  - Private citizens (often current or former employees) acting as whistleblowers can file a qui tam action
    - Receive a percentage of the recovery – 15% - 30%
  - Department of Justice
    - Can file a direct action
    - Can take over a whistleblower action

# KEY RISKS – FALSE CLAIMS ACT

- Civil penalties
  - Damages of up to three times the Government's actual damages
  - Fines of \$11,665 to \$23,331 per false claim (2020)
    - Amounts go up every year
- Criminal penalties of up to 5 years imprisonment and criminal fines
- Administrative penalties:
  - Suspension or debarment
  - Contract termination

## KEY RISKS – FALSE CLAIMS ACT

- Total recovery for FY 2020 was over \$2.2 billion
  - Over \$1.8 billion was in the health care industry
- Over \$1.68 billion was recovered through qui tam actions
- 722 new FCA actions were filed in FY 2020
  - 672 of them were qui tam actions
  - Qui tam relators recovered over \$309 million

CLE CODE #3

PA4000

# QUESTIONS?

Lori Ann Lange  
Peckar & Abramson, P.C.  
[llange@pecklaw.com](mailto:llange@pecklaw.com)