# PACIFIC NORTHWEST DEFENSE COALITION
# NORTHWEST AEROSPACE DEFENSE SYMPOSIUM

# GOVERNMENT CONTRACTS UPDATE – A DISCUSSION ON THE FAR & DFARS

**Jonathan A. DeMella**
**Davis Wright Tremaine LLP**
**Government Contracts Counseling & Litigation**

**May 4, 2017**

# False Claims Act Update

# False Claims Act, 31 U.S.C. § 3729

- Government's primary anti-fraud Weapon
- Prohibits presenting false documents or information to the Government for payment
- $5,000 - $11,000 per violation, treble damages
  - Presumption of loss rule for SBA-related fraud
- Three primary types
  - Direct False Claims (knowingly presenting a false claim, e.g., proposal, certified payroll)
  - False Statements
  - Reverse false claims (e.g., refund, silent in not telling the Government whole truth)
- Knowingly includes "deliberate ignorance" and "reckless disregard"
  - No such thing as innocent mistake
- Material - "having a naturally tendency to influence payment or receipt of money"
- FAR 52.203-13 (implement business ethics and compliance program, inform IG of credible evidence of any violation of civil or criminal fraud)

# *Escobar* – Implied Certification Theory of Liability Unanimously Upheld

- The Government argued that a failure to disclose a violation of a material statutory, regulatory, or contractual requirement in connection with the submission of payment would render the claim "false" under the FCA
- Court unanimously upheld "implied certification" theory of FCA liability on two conditions:
  - the claim for payment makes specific representations about the goods or services provided
  - the party's failure to disclose noncompliance with material statutory, regulatory or contractual requirements makes those representations misleading half-truths
- Implied certification: when a contractor submits a claim to the Government, the defendant "impliedly certified compliance with all conditions of payment."

# *Escobar* – Not All Violations are "Material"

- Court rejected the Government's "extraordinarily expansive" view of FCA liability regarding materiality:
  - The Government may not claim that "that any statutory, regulatory, or contractual violation is material so long as the defendant knows that the Government would be entitled to refuse payment were it aware of the violation."
- FCA's materiality standard looks to whether knowledge of the noncompliance would have *actually* affected the government's payment decision, not just whether it *could have* done so.
- Government's past behavior regarding payment in view of violation is a factor in determining materiality

# *Escobar* – Lower Court Response

- Since Escobar, lower courts more willing to consider motion to dismiss for failure by Government to plead materiality with specificity/particularity
- Summary judgment possible if Government/relator fails to offer evidence that Government's decision to pay would not have been different had it known of noncompliance
- *Escobar* increases focus on the Government's knowledge of alleged noncompliance – this bears upon intent of defendant
- DOJ still takes position that test for materiality is the "natural tendency" test – materiality is a flexible standard

# *Escobar* – Conclusions and Takeaways

- Affirmance of implied certification is not good for contractors
- New hurdle for FCA plaintiffs and Government on question of materiality is good for contractors
  - Continued payment of claims by the Government will afford contractors a materiality defense long resisted by DOJ and previously employed by the courts, largely in the context of contractor's intent to knowingly submit a false claim
- Definition of materiality remains unduly vague, and will likely lead to conflicting court decisions, more litigation

# Cybersecurity

# Basic Safeguarding of Contractor Information Systems, FAR 52.204-21

- Issued May 16, 2016 (effective date June 15, 2016)
- Adds FAR Subpart 4.19
- Applies to all acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf items, when a contractor's information system may contain Federal contract information
- Intent is to impose basic safeguarding measures as part of contractor's routine practice
- This is the starting point for compliance – 15 basic security controls
- Applies to covered contractor information systems, aimed at protecting covered contractor information
- Must flow down

# FAR 52.204-21 – Important Definitions

- “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
- “Covered contractor information system” means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.
- “Federal contract information” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

# FAR 52.204-21 - Minimum Security Controls

- Contractor must apply basic safeguarding requirements, which include, at a minimum, the following 15 security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(iii) Verify and control/limit connections to and use of external information systems.
(iv) Control information posted or processed on publicly accessible information systems.
(v) Identify information system users, processes acting on behalf of users, or devices.
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(xii) Identify, report, and correct information and information system flaws in a timely manner.
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
(xiv) Update malicious code protection mechanisms when new releases are available.
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed

# FAR 52.204-21 – Conclusions

- Requirements “reflective of actions a prudent business person would employ”
- Intent is that scope and applicability of rule be “very broad, because this rule requires only the most basic level of safeguarding”
- Rule is “just one step in a series of coordinated regulatory actions being taken or planned to strengthen protections of information systems”
- Lack of uniformity among agencies regarding rules, requirements
- Burden of compliance continues to shift to contractor
- Increased risk associated with noncompliance, data breach/loss

# FAR 52.204-21 – What May Be Coming

- Requirement for employee training
- Mandatory penetration testing
- Mandatory intrusion detection systems ($$)
- Mandatory encryption at rest (hard drives, thumb drives)
- Mandatory cyber-liability insurance

# Safeguarding Covered Defense Information and Cyber Incident Reporting, DFARS 252.204-7012

- DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”
- Contractor shall provide “adequate security” on all “covered contractor information systems”
- Covered contractor information systems shall be subject to the requirements in NIST SP 800-171, “Protecting Controlled Unclassified Information [“CUI”] in Nonfederal Information Systems and Organizations”
- Contractor shall implement NIST SP 800-171 “as soon as practicable,” but not later than December 31, 2017
- Rapid Reporting Requirement
- Cloud computing addressed in different rule

# Safeguarding Covered Defense Information and Cyber Incident Reporting, DFARS 252.204-7012

- *Covered defense information* means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls

- Some Categories of CUI: CTI, Critical Infrastructure, Emergency Management, Export Control, Financial, Geodetic Information, IS Vulnerability Information, Intelligence, Nuclear, Patent, Privacy, Procurement and Acquisition, Proprietary Business Information, SAFETY Act, Statistical

- "Controlled Technical Information"

  - Means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination

  - Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

- Contractor must "map" and identify appropriate security control in accordance with controlling guidance, including NIST SP 800-171 / FIPS 200

# Safeguarding Covered Defense Information and Cyber Incident Reporting, DFARS 252.204-7012

- Reporting Requirement:  Upon identification of “cyber incident”
  - Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein
  - Note that “cyber incident” not subject to uniform definition outside of Department of Defense

# Safeguarding Covered Defense Information and Cyber Incident Reporting, DFARS 252.204-7012

- Upon identification of "cyber incident" contractor shall:
  - Conduct review for evidence of compromise of covered defense information
  - Analyze covered contractor information systems that were part of the cyber incident
  - Rapidly report (*i.e.*, within 72 hours of discovery) cyber incidents to DOD at http://dibnet.dod.mil
  - Preserve and protect images of all known affected information systems for at least 90 days from submission of report
  - Upon request, contractor shall provide DoD with access to additional information and systems to conduct forensic analysis

# Cybersecurity - FAR and DFARS Comparison

- FAR more limited and basic – reasonable prudent business person
- DFARS mandates enhanced safeguarding
- FAR does not impose reporting, incident response, data collection requirements
  - Reporting and data collection proven to be most difficult for contractors
- FAR does not implement more rigorous NIST 800-171 requirements
- Upshot:  Build cybersecurity into ethics and compliance program
- Help from SBA for cybersecurity strategy for SBs?

# SBA All Small Mentor Protégé Program

# SBA Government-wide Mentor Protégé Program – 13 CFR 125.9

- Final Rule Effective August 24, 2016, 81 FR 48557
- Modeled on 8(a) program
- Application period opened October 2016, 147 All Small JVs approved to date
  - Online tutorial required (3400 views so far)
- Allows all small business protégés to joint venture with large business mentors without affiliation
  - Mentor-protégé joint ventures may qualify as a small business for any federal government contract or subcontract where the protégé qualifies as small for the size standard assigned to the procurement
- Applications are being processed very quickly (8 day average)

# SBA Government-wide Mentor Protégé Program – 13 CFR 125.9

- 8(a) applications processed through district offices, AS online
- 8(a)s can go through either program, compete for 8(a) contracts
- JVs may no longer be “populated”
- Generally, mentor can have 1 protégé, max of 3 at one time, applies to entire corporate structure
- Protégé – limit of 2 over a lifetime
- Protégé must be small in primary NAICS, but can qualify as small in secondary NAICS
  - SBA may approve second mentor if relationship will not compete or conflict with 1st MP relationship
  - Must demonstrate you have done work in secondary NAICS code

# SBA Government-wide Mentor Protégé Program – 13 CFR 125.9

- Relationship lasts three years, option for 3 year extension – six years is absolute cap
- Relationship reviewed annually to assess whether mentor is providing assistance as set forth in JV agreement
- Past performance of JV members will be considered, not limited to past performance of JV
- Protégé must perform 40% of work of JV, and they must report compliance
- Limitations on subcontracting – differences between SBA and FAR rules:
  - Similarly situated entities at first tier
  - New Services formula: shift from “labor cost” to “amount paid”
  - New Manufacturing formula: shift from “cost of manufacturing” to “amount paid”
  - According to SBA Director, follow FAR rule or request deviation until FAR Council catches up
- Mentor may own 40% of protégé, but should not appear to benefit mentor at protégé’s expense

# SBA Government-wide Mentor Protégé Program – 13 CFR 125.9

- Failure by mentor
  - Termination of agreement
  - Prohibition from being a mentor for two years
  - SBA may request CO to stop work
  - Debarment
- SBA is not reviewing JV agreements for All Small program, unlike 8(a) which still requires approval prior to award
- SBA expects COs will examine JV agreements more closely

# SBA Government-wide Mentor Protégé Program – 13 CFR 125.9

- JV Agreement – have an "overkill" mindset in meeting JV requirements
  - PM must be employee of protégé, and NOT a former employee of the mentor
  - Profits must be distributed commensurate with work performed
  - Requirement for itemization of equipment, facilities, and resources
- Agreement should focus on benefits to protégé
- Do as much as you can in your JV agreement to win if you are protested
- Have general provisions in JV agreement, execute addendum for each specific contract
- Each JV entity can receive 3 awards every 2 years

# SBA Government-wide Mentor Protégé Program – 13 CFR 125.9

- SBA anticipates heavily increased competition for set asides
- Strategic considerations
  - If LBC, is access to SB opportunities worth investment to find right partner
  - If SBC, will there be enough work if you don't have a partner

# Thank You

**Jonathan A. DeMella, Partner**
**Davis Wright Tremaine LLP**

**Jonathandemella@dwt.com**

**206.757.8338**

# FAR & DFARS Rules – Selected Updates from 2016-2017

# FAR Final Rule - Contractor Employee Internal Confidentiality Agreements or Statements

- Prohibits Government from contracting with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse
- Applies to all solicitations and contracts supported by FY 2015 or later funds; no exception for COTS items or acquisitions below micropurchase threshold
- Retroactive, COs are directed to modify existing contracts
- Effective January 19, 2017
- 82 FR 4717, FAR 3.901, 3.909, 52.203-18

# FAR Final Rule - Increase in SAT for Special Emergency Procurement Authority

- Simplified Acquisition Threshold for special emergency procurement authority increased from:
  - $300,000 to $750,000 within the United States
  - $1 million to $1.5 million Outside the United States
- Applies to acquisitions of supplies or services that, as determined by head of agency, are to be used to support a contingency operation or facilitate defense against or recovery from nuclear, biological, chemical, or radiological attack
- Effective January 13, 2017
- See changes at FAR 2.101, 13.003, 19.203, 19.502
- 82 FR 4716

# FAR Final Rule - Privacy Training

- Objective is to ensure that contractor employees complete initial and annual privacy training if the employees have access to a system of records, handle personally identifiable information (PII), or design, develop, maintain, or operate a system of records involving PII on behalf of the Government
- PII – “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See OMB Circular No. A-130, FAR 24.101)
- Employees must complete initial privacy training and annual privacy training thereafter

# FAR Final Rule - Privacy Training

- The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users.
- Applies to Contracts and subcontracts, including those at or below the SAT, as well as contracts and subcontracts for commercial items, including COTS items
- Effective January 19, 2017
- See 81 FR 93476, FAR 24.3, FAR 52.224-3

# FAR Final Rule – Payment of Subcontractors

- A reporting window of 14 days is added to FAR 52.242-5, Payments to Small Business Contractors, for prime contractors to report to the contracting officer an *untimely or reduced payment* made to their small business subcontractors.
  - *Reduced payment* means a payment that is for less than the amount agreed upon in a subcontract in accordance with its terms and conditions, for supplies and services for which the Government has paid the prime contractor
  - Untimely payment means a payment that is more than 90 days past due under the terms and conditions of a subcontract, for supplies and services for which the Government has paid the prime contractor.

# FAR Final Rule – Payment of Subcontractors

- Requires contracting officers to report to FAPIIS a contractor that has a history of three or more reduced or untimely payments to small business subcontractors within a 12-month period under a single contract that are *unjustified*
- These situations are not considered unjustified
  - Contract dispute on performance
  - Partial payment is made for amounts not in dispute
  - Payment is reduced due to past overpayments
  - Administrative mistake
  - Late performance by the sub leads to later payment by prime
- Applies to prime contractor payments made to first-tier small business subcontractors
- Applies to acquisitions  of commercial items, including COTS items
- Effective January 19, 2017
- See 81 FR 93481, FAR 42.1503, FAR 52.212-5, FAR 52.245-5

# FAR Final Rule – Small Business Subcontracting Improvements

- Rule aimed at providing a Government wide policy on small business subcontracting.
- Prime contractors must make good faith efforts to utilize their proposed small business subcontractors during performance of a contract to the same degree the prime contractor relied on the small business in preparing and submitting its bid or proposal. To the extent a prime contractor is unable to make a good faith effort to utilize its small business subcontractors as described above, the prime contractor is required to explain, in writing, within 30 days of contract completion, to the contracting officer the reasons why it is unable to do so.
  - Potential for liquidated damages
- Prime contractors restricted from prohibiting a subcontractor from discussing payment or utilization matters with the contracting officer.
- Affords COs greater discretion to require from prime (even a small business) a subcontracting plan
- Effective November 1, 2016
- 81 FR 45833, FAR 1.106, 2.101, 15.304, 19.301-2, 19.305, 19.701, 19.702, 19.703, 19.704, 19.705-1, 19.705-2, 19.705-4, 19.705-6, 52.212-5, 52.213-4, 52.219-8, 52.219-9, 52.244-6

# FAR Final Rule – Sole Source Contracts for Women-Owned Small Businesses

- Grants contracting officers the authority to award sole source contracts to economically disadvantaged women-owned small business (EDWOSB) concerns and to WOSB concerns eligible under the WOSB Program
- Sole source authority can only be used where a contracting officer conducts market research in an industry where a WOSB or EDWOSB set-aside is authorized, and cannot identify two or more eligible EDWOSB or WOSB concerns that can perform at a fair and reasonable price, but identifies one WOSB or EDWOSB that can perform
- Sole source authority is limited to contracts valued at $6.5 million or less for manufacturing contracts and $4 million or less for all other contracts
- Effective September 30, 2016
- 81 FR 67735, FAR 2.101, 4.803, 6.302-5, 18.117, 19.15, 52.212-5, 52.219-29, 52.219-30

# FAR Final Rule – Information on Corporate Contractor Performance and Integrity

- Requires that the FAPIIS include, to the extent practicable, information on any parent, subsidiary, or successor entities to a corporation in a manner designed to give the acquisition officials using the database a comprehensive understanding of the performance and integrity of the corporation in carrying out Federal contracts and grants
- Requires approximately 1 submission per year, with a 3 year lookback
- Applies to commercial items, including COTS items
- No exemption for small entities
- Effective April 6, 2016
- 81 FR 11988, FAR 1.106, 4.1202, 4.1804, 9.104-6, 9.105-1, 22.1006, 52.204-8, 52.204-20 52.212-3

# Final Rule (DFARS) – Display of Hotline Posters

- Rule amends DFARS to consolidate multiple hotline posters into one DoD fraud, waste, and abuse hotline poster (prepared by DoDIG) that delineates multiple reportable offenses
- For contracts performed outside of the United States, CO may provide contractor an alternative means of notifying contractor personnel of DoD Hotline program
- Effective October 21, 2016
- 81 FR 73005, DFARS 203.1003, 252.203-7004