

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



WELCOME ATTENDEES

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

False Claims Act: Investigations, Enforcement, and Litigation Trends

Tully McLaughlin

Jason Crawford

Mana Lombardo

Nkechi Kanu

Agenda

- *DOJ Enforcement Trends and Developments: What They Mean for Investigation and Litigation Strategy*
- *The Continuing Emphasis on Materiality in the Wake of Escobar*
- *Case Developments and Impacts*

2017 FCA Recoveries

- Over \$3.7 billion recovered in FCA settlements or judgments in 2017
- Eight consecutive years of recovery exceeding \$3 billion



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Number of New FCA Matters

- 799 new FCA cases filed in 2017
- Eighth consecutive year where over 700 new cases were filed



Qui Tam Activity Consistent

- *Qui tam* actions continue to be the majority of suits filed under FCA
 - FY 2017: Whistleblowers initiated approximately 84% of the FCA cases
 - average of more than 12 new cases every week
 - 7th consecutive year in which relators filed 600 or more matters

Qui Tam Recoveries High

- Over \$425 million recovered from suits where government declined to intervene
 - 11% of total FCA recoveries in FY 2017
 - 2nd highest recovery in non-intervened cases



Expanded Scope of FCA Liability

- FCA liability is being applied to new classes of defendants
 - Third-party FCA liability to surety companies, private equity sponsors, and auditors
 - *U.S. ex rel. Scollick v. Narula*
 - No. 14-CV-01339-RCL, 2017 WL 3268857 (D.D.C. July 31, 2017).
 - *U.S. ex. rel. Medrano v. Diabetic Care RX, LLC*
 - No. 15-CV-62617 (S.D. Fla. Feb. 16, 2018)
- Opioid Crisis

DOJ Policies - Granston Memo

- Background: per 31 USC § 3730(C)(2)(A), the government has the right to dismiss a *qui tam* action over the objections of the relator
 - but less than 1% of cases are dismissed under this provision
- January 2018: Granston memo provides bases for DOJ lawyers to seek dismissal of non-intervened *qui tam* cases that “lack substantial merit”

DOJ Policies - Granston Memo (cont'd)

Seven factors to guide dismissal:

1. The legal theory in the complaint is inherently defective or the factual allegations are frivolous;
2. The relator is providing only duplicative information and dismissal would prevent an “unwarranted windfall” to the relator
3. The *qui tam* action threatens to interfere with agency policies and programs;
4. The case may lead to an unfavorable precedent or may interfere with DOJ’s ongoing litigation;
5. Dismissal is necessary to protect classified information or matters of national security;
6. The Department’s costs are expected to exceed any expected gains;
7. The relator has obstructed the government’s ability to adequately investigate the claims.

DOJ Policies - Granston Memo

(cont'd)

- Impact of Granston Memo
 - Increase in government dismissals?
 - More leverage for defendants to convince DOJ not to intervene?
 - Increase in relators abandoning those cases that could involve the enumerated factors?

DOJ Policies - Brand Memo

- January 2018: agency guidance documents DO NOT create binding requirements not in existing statute or regulation
 - noncompliance with guidance documents is not a basis for proving violations of the FCA
- Impact: stronger grounds to challenge FCA suit when DOJ's evidence is based in guidance materials

Increased Penalties

- Penalties have nearly doubled to \$11,181 to \$22,363 for FCA violations after Nov. 1, 2015
 - More and more cases are subject to the higher penalty amounts
- Penalties will be adjusted annually for inflation
- Potential for more 8th amendment challenges

Trends to Monitor

- Number of FCA cases and recovery amounts remain high under new administration
- Higher penalties continue to loom
- DOJ guidelines may signal a shift
 - Federal FCA legislation and DOJ enforcement history have disfavored contractors for years
 - DOJ policies this year may reign in relators and articulate some boundaries

“There is no shortage of FCA allegations that we can pursue, so we want to focus our attention on the most worthy of cases.”

--Deputy Associate Attorney General Stephen Cox (Feb. 2018)

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Life After *Escobar*



Universal Health Services, Inc. v. United States ex rel. Escobar, 136 S.Ct. 1989 (2016)

Life After *Escobar*

- *Escobar* validated implied certification theory of liability—*i.e.*, where a contractor requests payment but fails to disclose noncompliance with material requirements
- Imposed a “rigorous” materiality standard
- Laid out several factors that might contribute to a finding of materiality, including evidence that the government consistently pays claims in the face of noncompliance

An Oft-Cited Footnote

- In the two years since the decision, nearly 300 opinions have cited *Escobar*, including almost every court of appeals
- *Escobar* 136 S. Ct. at 2004 n.6: materiality test not too fact intensive for dispositive motions
- A number of circuits have been willing to affirm dismissals on the basis of materiality at MTD or SJ stage

Affirming SJ Dismissal

- *U.S. ex rel. McBride v. Halliburton*, 848 F.3d 1027 (D.C. Cir. 2017)
 - DCAA investigated allegations of inflated headcount data and did not disallow costs
- *U.S. ex rel. Kelly v. Serco, Inc.*, 846 F.3d 325 (9th Cir. 2017)
 - Government knew cost reports did not comply with earned value management guidelines and still accepted reports
- *Abbott v. BP Exploration & Prod.*, 851 F.3d 384 (5th Cir. 2017)
 - Government aware of non-compliance with engineering regulations yet allowed defendant's continued drilling

Affirming MTD

- In *U.S. ex rel. Folliard v. Comstor Corp.* (DDC 2018), relator alleged that defendants violated the FCA by selling non-TAA compliant products
- Held: Relator failed to adequately plead sufficient facts to show that sale of TAA compliant products was material to government's payment decision



Affirming MTD, cont.

- *D'Agostino v. ev3 Inc.*, 845 F.3d 1 (1st Cir. 2016)
 - alleged false statements to FDA not material because FDA did not withdraw device approval after allegations surfaced
- *U.S. ex rel. Petratos v. Genentech Inc.* 855 F.3d 481 (3d Cir. 2017)
 - failure to plead materiality because FDA continued to approve drug after allegations surfaced

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Impact of Intervention Decision on Material Analysis

- *In Petratos*, DOJ's decision not to intervene was a factor that weighed against a finding of materiality
- But, in *U.S. ex rel. Omar Badr v. Triple Canopy*, 857 F.3d 174 (4th Cir. 2017), DOJ's decision to intervene was considered evidence of materiality

Who Knew and When Did They Know It

- In *U.S. ex rel. Campie v. Gilead Scis., Inc.*, 862 F.3d 890 (9th Cir. 2017), relator alleged that defendant falsified information about drug suppliers to gain FDA approval
- Defendant argued that gov't continued to make payments despite awareness of violations
- Ninth Circuit: too many factual questions to resolve at the MTD stage because the parties disputed what the government knew and when

Escobar Redux?

- April 16, 2018: the Supreme Court called for the views of the Solicitor General as to whether the Court should grant cert in *Campie*
- “Question Presented: Whether an FCA allegation fails when the Government continued to approve and pay for products after learning of alleged regulatory infractions and the pleadings offer no basis for overcoming the strong inference of immateriality that arises from the Government’s response. ”

Developments in the Law

- Does SOL tolling provision apply when the government declines to intervene?
- What constitutes an “obligation” under the reverse FCA?
- Does the “reasonable interpretation defense” still preclude a finding of scienter?
- How broad is the scope of the government-action bar?
- Is statistical sampling an appropriate methodology for establishing FCA liability and damages?

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

**Statute of Limitations: Does SOL
tolling provision apply when the
government declines to intervene?**



Does SOL tolling provision apply when the government declines to intervene?

“A civil action under section 3730 may not be brought—

(1) more than 6 years after the date on which the violation of section 3729 is committed, or

(2) more than 3 years after the date when facts material to the right of action are known or reasonably should have been known by the official of the United States charged with responsibility to act in the circumstances, but in no event more than 10 years after the date on which the violation is committed, whichever occurs last.”





DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Does SOL tolling provision apply when the government declines to intervene?

- 4th and 10th Circuits: § 3731(b)(2) - tolling provision - only applies if the Gov't has intervened in the action.
 - *U.S. ex rel. Sanders v. N. Am. Bus Indus., Inc.* 546 F.3d 288 (4th Cir. 2008) (“Congress intended Section 3731(b)(2) to extend the FCA's default six-year period only in cases in which the Government is a party, rather than to produce the bizarre scenario in which the limitations period in a relator's action depends on the knowledge of a nonparty to the action.”)
 - *U.S. ex rel. Sikkenga v. Regence Bluecross Blueshield of Utah*, 472 F.3d 702 (10th Cir. 2006) (“Surely, Congress could not have intended to base a statute of limitations on the knowledge of a non-party.”)



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Does SOL tolling provision apply when the government declines to intervene?

- In *U.S. ex rel. Hunt v. Cochise Consultancy, Inc.*, 887 F.3d 1081 (11th Cir. April 11, 2018), relator disclosed to authorities information providing the underpinning to his *qui tam* case while agents interviewed him about a different fraud scheme.
- Relator brought action more than 6 yrs. after alleged conduct but within 3 yrs. of his disclosure to authorities.
- Gov't declined to intervene.
- District court dismissed case as time barred holding that relator could not take advantage of § 3731(b)(2) given Gov't decision not to intervene.



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Does SOL tolling provision apply when the government declines to intervene?

- 11th Circuit reversed, finding that *“nothing in § 3731(b)(2) says that its limitations period is unavailable to relators when the Government declines to intervene.”*
- Rejected defendants’ argument that allowing relator to rely on tolling provision when Gov’t declined to intervene would lead to an “absurd result” because limitations period would depend on the knowledge of a nonparty.
 - Court found that even if Gov’t declines to intervene, it still “remains the real party in interest and retains significant control over the case.”

Does SOL tolling provision apply when the government declines to intervene?

- In finding that a relator can avail itself of 3731(b)(2), 11th Circuit joined 9th Circuit and split with the 4th and 10th Circuits that have held that the second prong of the FCA's SOL applies only to the Gov't.
- 11th Circuit also held that it is the knowledge of a Gov't official, not the relator, that triggers the limitations period – split from 9th Circuit's holding in *United States ex rel. Hyatt v. Northrop Corp.*, 91 F.3d 1211 (9th Cir. 1996)

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Reverse FCA: What constitutes an “obligation” to pay money to the Government?

What constitutes an “obligation” to pay money to the Government?

- 3729(a)(1)(G) – known as the reverse FCA – provides liability when one “knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government.”
- Liability requires the existence of an “obligation” to pay money to the Gov’t, which the 2009 FERA amendments to the FCA defined as:

“[A]n established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment.”

What constitutes an “obligation” to pay money to the Government?

U.S. ex rel. Petras v. Simparel, Inc., 857 F.3d 497 (3d Cir. 2017)

- Relator alleged that Simparel improperly avoided obligation to pay accrued dividends to an investor after it had been placed into receivership and was being operated by SBA.
- Court found that there was no “obligation” to repay under the reverse FCA because payment was contingent on either the board’s declaration of dividends or the company’s liquidation.

U.S. ex rel. Barrick v. Parker-Migliorini Int’l, LLC, 878 F.3d 1224 (10th Cir. 2017)

- Relator alleged that PMI avoided paying inspection fees to the USDA by providing inaccurate destinations for their meat exports.
- Court found that there was no established obligation to pay inspection costs because payment depended on a future discretionary act by a third party – PMI’s supplier needed to report specific information to the USDA.

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Scienter: Does the “reasonable interpretation defense” still preclude a finding of knowledge?



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Does the “reasonable interpretation defense” preclude a finding of knowledge?

- Courts have held that the reasonable interpretation of an ambiguous regulation precludes a finding of scienter.
- ***U.S. ex rel. Purcell v. MWI Corp.*, 807 F.3d 281 (D.C. Cir. 2015), cert. denied, 137 S. Ct. 625, 196 L. Ed. 2d 516 (2017)**
 - Defendant did not act knowingly where government failed to warn defendant away from its otherwise facially reasonable interpretation of an undefined and ambiguous term.
- ***U.S. ex rel. Donegan v. Anesthesia Assoc. of Kansas City*, 833 F.3d 874 (8th Cir. 2016)**
 - Defendant's reasonable interpretation of the ambiguous term “emergence” “belie[d] the scienter necessary to establish a claim of fraud under the FCA.”



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Does the “reasonable interpretation defense” preclude a finding of knowledge?

U.S. ex rel. Phalp v. Lincare Holdings, 857 F.3d 1148 (11th Cir. 2017)

- Trial court dismissed action, finding that whenever a defendant can show that its conduct was consistent with a reasonable interpretation of an ambiguous regulation, the conduct was not a knowing violation.
- 11th Circuit affirmed dismissal, but rejected the district court’s knowledge standard, explaining that:
 - It would permit post hoc reasonable interpretations that shielded defendants from liability.
 - the proper approach is “whether the defendant actually knew or should have known that its conduct violated a regulation in light of any ambiguity at the time of the alleged violation.”

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Government Action Bar

The background of the slide features a vertical image of an iceberg. The top portion shows the jagged, white peak of the iceberg above the water's surface. Below the surface, the water is a deep blue, and three divers in black gear are visible. One diver is in the foreground, swimming horizontally, while two others are further back and higher up. The overall scene is serene and somewhat mysterious, reflecting the 'uncharted waters' theme.

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

How broad is the government action bar?

- The “Government-action bar” —31 USCA § 3730(e)(3)— prohibits a relator from bringing a qui tam suit “based upon allegations or transactions which are the subject of a civil suit ... in which the Government is already a party.”
- ***U.S. ex rel. Bennett v. Biotronik, Inc.*, 876 F.3d 1011 (9th Cir. 2017)**
 - Gov’t action bar applies even where the original action is no longer pending
 - Gov’t does not cease to be a party even after the action has concluded.
 - When the Gov’t intervenes in an FCA case, it “becomes a ‘party’ to the suit as a whole,” “unsettled claims and all.”

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Statistical Sampling

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Is statistical sampling an appropriate methodology for establishing FCA liability?

U.S. ex rel. Michaels et al. v. Agape Senior Community Inc., 848 F.3d 330 (4th Cir. 2017).

- Dismissed interlocutory appeal as “improvidently granted” in light of the panel’s view that statistical sampling is an evidentiary issue, rather than a pure question of law.
- Concluded that the U.S. attorney general possesses an absolute veto power over voluntary settlements in qui tam actions – even in non-intervened cases.

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Jason Crawford

(202) 624-2562

jcrawford@crowell.com

Nkechi Kanu

(202) 624-2872

nkanu@crowell.com

Mana Lombardo

(213) 443-5563

melombardo@crowell.com

Tully McLaughlin

(202) 624-2628

bmclaughlin@crowell.com

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Looking Back and Forward – 2017 M&A Highlights and Trends to Watch

Jim Stuart

Karen Hermann

Judy Choi

Tim Garnett, Avascent Consulting

Market Trends

- 2017 Highlights
- 2018
 - Headlines to Date
 - Trends to Watch
 - Emerging Market Areas
 - Market Risks

Novation – FAR Requirements

42.1204 Applicability of novation agreements.

- (a) [41 U.S.C. 6305](#) prohibits transfer of Government contracts from the contractor to a third party. The Government may, when in its interest, recognize a third party as the successor in interest to a Government contract when the third party's interest in the contract arises out of the transfer of—
- (1) All the contractor's assets; or
 - (2) The entire portion of the assets involved in performing the contract.
- (See [14.404-2\(l\)](#) for the effect of novation agreements after bid opening but before award.) Examples of such transactions include, but are not limited to—
- (i) Sale of these assets with a provision for assuming liabilities;
 - (ii) Transfer of these assets incident to a merger or corporate consolidation; and
 - (iii) Incorporation of a proprietorship or partnership, or formation of a partnership.
- (b) A novation agreement is unnecessary when there is a change in the ownership of a contractor as a result of a stock purchase, with no legal change in the contracting party, and when that contracting party remains in control of the assets and is the party performing the contract. However, whether there is a purchase of assets or a stock purchase, there may be issues related to the change in ownership that appropriately should be addressed in a formal agreement between the contractor and the Government (see [42.1203\(e\)](#)).

Novation Process

- Timing
 - Post-Closing Requirement
 - Impacts Deal Certainty
 - Subcontracts Pending Novation
- Change in Corporate Entity Structure
- Contents of Novation Package
 - Audited Financial Statements
 - Corporate Seal / Board Documents

Novation – Special Challenges

- Intercompany Transactions
- Agency Coordination and Unique Requirements
- Redundant IDIQ Vehicles
- Pending Bids
- Parent Guarantees

Identifying Risks

- Determining the scope of diligence
 - What is the business case?
- Prior deals and residual issues
 - Lingering novations
- Organizational conflicts of interest
 - Self-diligence
 - Timing
- Small business matters
 - Impact on prospective business
 - Legacy compliance questions

Identifying Risks

- IP and Data Rights
 - IP/data rights clauses in target's contracts
 - Source of funds to develop software/products
- Supply Chain
 - Domestic preference requirements
 - Detection and avoidance of counterfeit parts
 - Flowdowns, reps and certs
- Cybersecurity and information safeguarding
 - DFARS safeguarding clause
 - Other restrictions/standards
- Attorney-Client Privilege Issues

Mitigation of Risk

- Transaction Risk Insurance
 - Not useful for “known” risks
 - Must meet underwriter’s requirements
 - Heightened diligence for certain risks and industries
- Indemnification Procedures
 - Who will control?
 - Allocation of Risk

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Judy Choi

(202) 624-2954

jchoi@crowell.com

Karen Hermann

(202) 624-2722

khermann@crowell.com

Jim Stuart

(202) 624-2865

jstuart@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Q&A with Emily Murphy, GSA Administrator

Rob Burton

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Brace for Impact – Protest Reform that Could Affect Your Business

Anuj Vohra

Christian Curran

James Peyster

Mark Ries

Rob Sneckenberg

809 Panel Recommendations

Volume 1 Recommendations Affecting Protests

- Solicitations not required for “Lanes 1 and 2”
- Sole source SBIR awards immune from protest
- Foreshadowing – protests have become a feedback tool

Protest Reform Recommendations Under Consideration

- Transparency – Release entire contract file at award
- Forum – DoD tribunal only
- Decisional Timing – 10 days from start to finish(!)
- Grounds – Sole basis: “good business decision?”
- Judicial Review – Appellate review only at CAFC
- Standing – Replace interested party with first-to-file bounty
- Remedies – Bounty system
 - No more CICA Stay
 - No more corrective action
 - Extend “loser pays” pilot program

Enhanced DoD Debriefings

- What are they?
 - Contractors now have two business days following initial debriefing to submit additional questions
 - DoD must respond in writing in five days; protest clock does not run until responses received
- When do they apply?
 - Apply to post-award debriefings in accordance with FAR 15.506(d)
- Do they provide different information?
 - No—changes do not impact the substance of what can be provided
- How do I use them to my advantage?
 - Potential for more information/clarification to inform protest decisions
 - More time to analyze situation before protesting

New GAO Rules and Regulations

- New rules effective May 1, 2018
- Formal Roll-Out of GAO’s Electronic Protest Docketing System (“EPDS”)
 - \$350 filing fee for filing GAO protests (previously free)
 - Filing through EPDS serves as instant agency notice for CICA Stay of Performance
- Timing Clarification for Certain Solicitation Protests
 - Protest of amendment to solicitation terms must be filed before next proposal submission deadline or within 10 days of announcement if no new submission deadline
- Assorted Minor Tweaks
 - Right to request redacted version of any protected document
 - Additional notice requirements for CICA Stay overrides
 - Additional briefing requirements for protest cost-recovery disputes

Enhanced DoD Debriefings

- What are they?
 - Contractors now have two business days following initial debriefing to submit additional questions
 - DoD must respond in writing in five days; protest clock does not run until responses received
- When do they apply?
 - Apply to post-award debriefings in accordance with FAR 15.506(d)
- Do they provide different information?
 - No—changes do not impact the substance of what can be provided
- How do I use them to my advantage?
 - Potential for more information/clarification to inform protest decisions
 - More time to analyze situation before protesting

Significant Developments—Protest Filings/Results

GAO Bid Protest Statistics

	FY2017	FY2016	FY2015	FY2014	FY 2013
Cases Filed	2596 (down 7%)	2789 (up 6%)	2639 (up 3%)	2561 (up 5%)	2429 (down 2%)
Cases Closed	2672	2734	2647	2458	2538
Merit (Sustain + Deny) Decisions	581	616	587	556	509
Number of Sustains	99	139	68	72	87
Sustain Rate	17%	23%	12%	13%	17%
Effectiveness Rate	47%	46%	45%	43%	43%
ADR (cases used)	81	69	103	96	145
ADR Success Rate	90%	84%	70%	83%	86%
Hearings	1.70% (17 cases)	2.51% (27 cases)	3.10% (31 cases)	4.70% (42 cases)	3.36% (31 cases)

Lots of Corrective Action!



DIVING INTO UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Significant Developments— Decisions of Note

OCI Waivers

- *CACI, Inc.-Federal; General Dynamics One Source, LLC, B-413860.4 et al.*, Jan. 5, 2018, 2018 CPD ¶ 17
 - FAR 9.503: “Any request for waiver must be in writing, shall set forth the extent of the conflict, and requires approval by the agency head or a designee”
 - Waiver upheld, even though (1) agency denied OCI existed; (2) prior contract clause specifically called future work an OCI; and (3) agency waived OCI only after award
- Note: Unfair Competitive Advantage (UCA) concerns not OCIs and *cannot* be waived. *Northrop Grumman Systems Corp.*, B-412278.7, .8, Oct. 4, 2017, 2017 CPD ¶ 312

Cybersecurity Protests

- *First Financial Associates, Inc.*, B-415713, .2, Feb. 16, 2018, 2018 CPD ¶ 76
 - GAO upheld agency determination that proposed 12-hour timeline for data breach notification was not sufficiently “expeditious”
- Draft DoD Guidance for Evaluating Contractor Cybersecurity, including Implementation of NIST SP 800-171
 - Regulations.gov, DARS-2018-0023; Comments Due by May 31



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



QUESTIONS?

Christian Curran

(202) 624-2543

ccurran@crowell.com

James Peyster

(202) 624-2603

jpeyster@crowell.com

Mark Ries

(202) 624-2794

mries@crowell.com

Rob Sneckenberg

(202) 624-2874

rsneckenberg@crowell.com

Anuj Vohra

(202) 624-2502

avohra@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Under Scrutiny: Contractors and Cybersecurity

Paul Rosen

Evan Wolff

David Bodenheimer

Michael Gruden

Navigating the Regulatory Seas: Information Security & Privacy Risk

- **Navigating Government Contracts
Information Security & Privacy Risk**
 - Federal & Global Cyber Risks and Regulations
- **Navigating IoT Cyber Threats & Risks**
 - Where do they start? Or End?
- **Navigating “Ordinary” Information Security
& Privacy Risk**
 - Legal Principles, Information Sharing, and Incident Preparation/Response



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Navigating Government Contracts Information Security & Privacy Risk

Federal & Global Cyber Risks and Regulations



Current Threat Environment

- Data breaches caused by third parties are increasing
- Nearly 50% of breaches are the result of hacking
- Almost 70% of breaches take 30 days or longer to detect
- 73% of breaches conducted by outsiders
- PII, payment, medical and credential data categories are most compromised



DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (OCT 2016)

- Incorporated into all Department of Defense (DoD) contracts to protect sensitive Government information except exclusively off-the-shelf (COTS) items
- 3 Core Requirement of Clause
 - (1) Safeguarding Covered Defense Information (CDI)
 - (2) Flowdown Clause to Subcontractors
 - (3) Cyber Incident Reporting
- December 31, 2017 Implementation Deadline

DFARS Safeguarding Requirements

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

- If Contractor processes, stores or transmits CDI on its information systems, it must implement “adequate security” on those systems to protect CDI
- Contractor achieves “adequate security” by implementing all 110 controls in NIST SP 800-171
 - Includes System Security Plans (SSPs) and Plans of Action and Milestones (POAMs)
 - DoD may use SSPs and POAMs as Evaluation Factors and consider in Source Selection Decisions

Controlled Unclassified Information (CUI) Program, 32 C.F.R. § 2002

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

- What is Controlled Unclassified Information (CUI)?
 - Categorized by the National Archives and Records Administration (NARA) and listed in the CUI Registry
 - Common CUI Categories arising in Government Contracting include:
 - Controlled Technical Information
 - Export Control Information
 - Privacy Information such as PII and Health Data
 - Procurement and Acquisition Information
 - Proprietary Business Information

DFARS Subcontracting Flowdown Requirements

- Subcontracting Requirements
 - Prime must flowdown the Clause without alteration to subs whose performance requires use of CDI
 - Prime must also require subs to:
 - (1) Notify Prime when submitting NIST SP 800- 171 variance request to DoD CIO; and
 - (2) Provide Prime Contractor with DoD incident report number upon cyber incident occurrence

DFARS Cyber Incident Reporting

- Cyber Incident Reporting Requirements
 - Contractor must report cyber incidents that either
 - “affect” CDI or any information system where CDI resides; OR
 - affect ability to provide operationally critical support
 - Contractor must report through DIBNet portal within 72 hours of discovery
 - Contractor must preserve and protect images of all information systems and relevant monitoring/packet capture data known to be affected for 90 days from date of reporting



Recent DFARS Cyber Developments

- Draft NIST SP 800-171A, “Assessing Security Requirements for Controlled Unclassified Information” (FEB 2018)
 - Provides sample SSPs and POAMs
 - Requests a greater level of detail
 - Encourages organization to document CUI information types processed, stored, or transmitted by a system
 - Directs organization to provide detailed narrative that describes each system component within the system environment
 - Mapping tables and guidance in Appendices

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Recent DFARS Cyber Developments

- DoD Updates to DFARS Safeguarding Clause Frequently Asked Questions (FAQs) (APR 2018), highlights include:
 - Unless prohibited by FAR/DFARS, all costs associated with compliance of DFARS 252.204-7012 are allowable.
 - May require contractors to identify and include POAMs for NIST SP 800-171 security controls NOT implemented at the time of award.
 - May require contractor to self-certify compliance with DFARS Clause 252.204-7012, including implementation of NIST SP 800-171.
 - Government may consider SSPs and POAMs when making overall risk management decision concerning contract award.

FAR Cyber Clause & Pending Developments

- FAR 52.204-21 (JUN 2016), Basic Safeguarding of Covered Contractor Information Systems
 - Mandatory in all contracts
 - Requires protection via 17 controls pulled from NIST SP 800-171
- Pending FAR Cybersecurity Clause
 - Pending FAR clause focused on Controlled Unclassified Information
 - Expected to largely mirror DFARS Safeguarding Clause
 - Would have same Safeguarding and Cyber Incident Reporting requirements
 - Expected to be proposed in the next few months

Federal Systems & Federal Information

- FISMA (2014 revision)
 - Increased accountability, reporting and oversight for data security and privacy
- Revised OMB Circular A-130 (July 28, 2016)
 - Data security and privacy are “crucial elements of a comprehensive, strategic, and continuous risk-based program”
 - Agency contracts must “enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information”
- Privacy Training Requirement, FAR Subpart 24.3 (Dec. 20, 2016; eff. Jan. 19, 2017)
 - Applies to all who work with Privacy Act systems of records and federal PII, with flowdown requirement
 - Specified training requirements include Privacy Act, working with federal PII, incident response, and potential civil and criminal consequences for violations

General Data Protection Regulation (GDPR)

European Legislation with Extraterritorial Effects

- GDPR will be effective May 25, 2018
- Harmonizes European data protection legislation
- Directly applies to all EU Member States
- Builds on existing legal concepts
- Strengthens rights of individuals
- Fines up to 4% total worldwide annual revenue or € 20M (\$23.7M currently), whichever is higher



General Data Protection Regulation (GDPR)

- GDPR applies if:
 - Establishment is operating in the EU, or
 - Not based in the EU but either
 1. Offering goods or services to EU-based individuals; OR
 - Mere accessibility through website or providing email address or contact details is **NOT** sufficient
 - EU language, payment in Euros **IS sufficient**
 2. Monitoring their behavior
 - e.g., Using cookies to track & create consumer profile (analyzing/predicting preferences, etc.)

Navigating IoT Cyber Threats & Risks

Where Do They Start? Or End?



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)





Why is IoT a Cyber Target?

- **It's Big!**

- **8.4 Billion Devices**
 - (2017)
- **20.4 Billion Devices**
 - (2020)

- **It's Lucrative!**

- **\$7 Trillion (2020)**
- **\$11 Trillion (2025)**

- **It's Everywhere!**

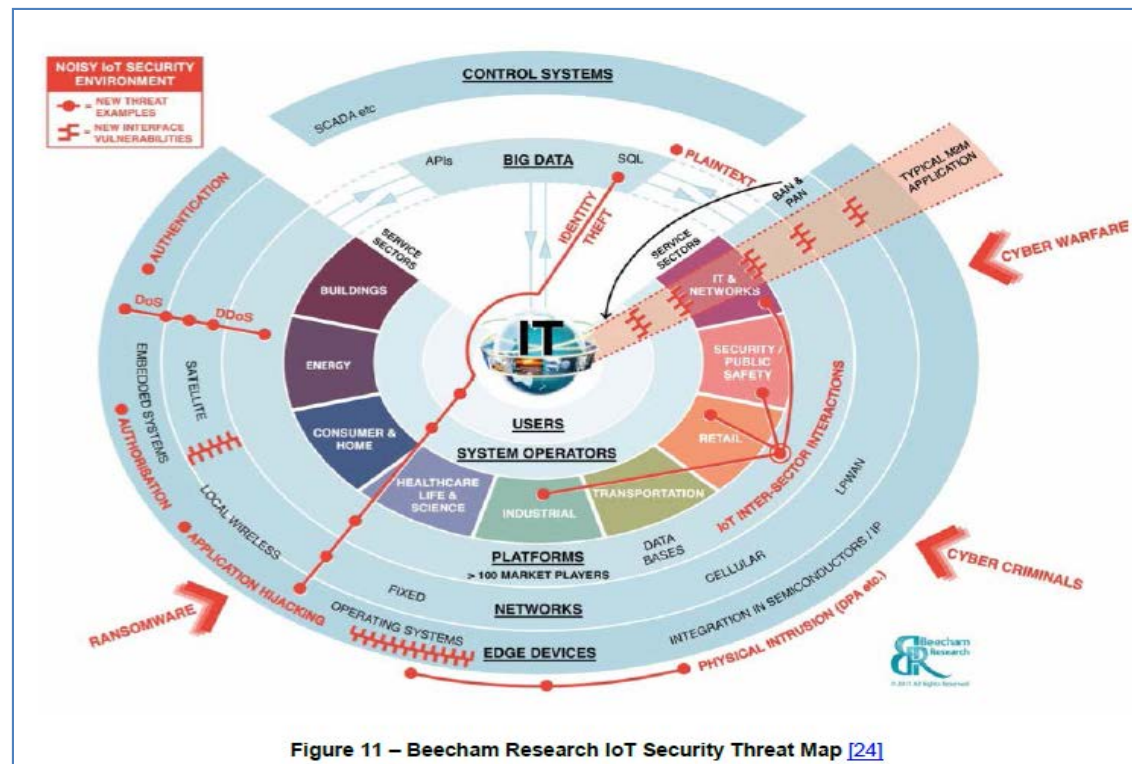
- **Smart-Everything**
- **Cars, Toasters, Pills, Buildings, Phones, Shoes**





IoT Cyber Threat Map

Where the Scary Things Are



- **Multiple Sectors:** Industrial, Health, Retail, Energy, Home
- **Multiple Devices:** Cars, phones, thermostats, drones, fridge
- **Multiple Networks:** Satellites, Cellular, Local Wireless, LPWAN
- **Multiple Edge Devices:** SCADA, embedded systems, operating systems

IoT Threats in the News



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Stopping Self-Driving Cars From
Becoming Cybersecurity Weapons

Forbes

IoT security for healthcare is in critical
condition **NETWORKWORLD**
FROM IDG

How my fridge caused hundreds
of websites to crash

HÉLÈNE CHAUVEAU | HEAD OF EMERGING RISKS AT AXA

IoT Gadgets: Exploring the New Sources of
Discoverable Evidence **Legaltech news**

Agencies' approach to IoT security
highlights differences in cybersecurity
approach 

The Internet of Things: The security
crisis of 2018? **information age**

IoT Cyber Risks: What's Bugging the Feds?

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Sen. Mark Warner (VA)

“Additionally, the sheer number of IoT devices – expected to exceed 20 billion devices by 2020 – has enabled bad actors to launch **devastating Distributed Denial of Service (DDoS) attacks.**” [S. 1691 Fact Sheet]

Rep. Jerry McNerney (CA)

“Security vulnerabilities in IoT devices are likely to pose **threats to our national security** and endanger our nation’s economy.” [comments on H.R. 1324, the Securing IoT Act]

Government Accountability Office

“For example, in 2016, **hundreds of thousands of weakly-secured IoT devices were accessed and hacked**, disrupting traffic on the Internet.” [GAO-17-75]

National Security Telecommunications Advisory Committee

“The **threat will only increase** as the number and type of IoT devices grow and as such devices become more autonomous, capable, and ubiquitous.” [NSATC Report on Internet & Communications Resilience]

Department of Homeland Security

“IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating **substantial safety and economic risks.**” [Strategic Principles for Securing the Internet of Things]

IoT National Security Threats

Department of Defense – Networks & Military Technology

Mission Sabotage

- Electrical system attack
- Knock out communications

Equipment Sabotage

- Insider threat to utilities
- Flood dry dock & sink ship

Security Breach

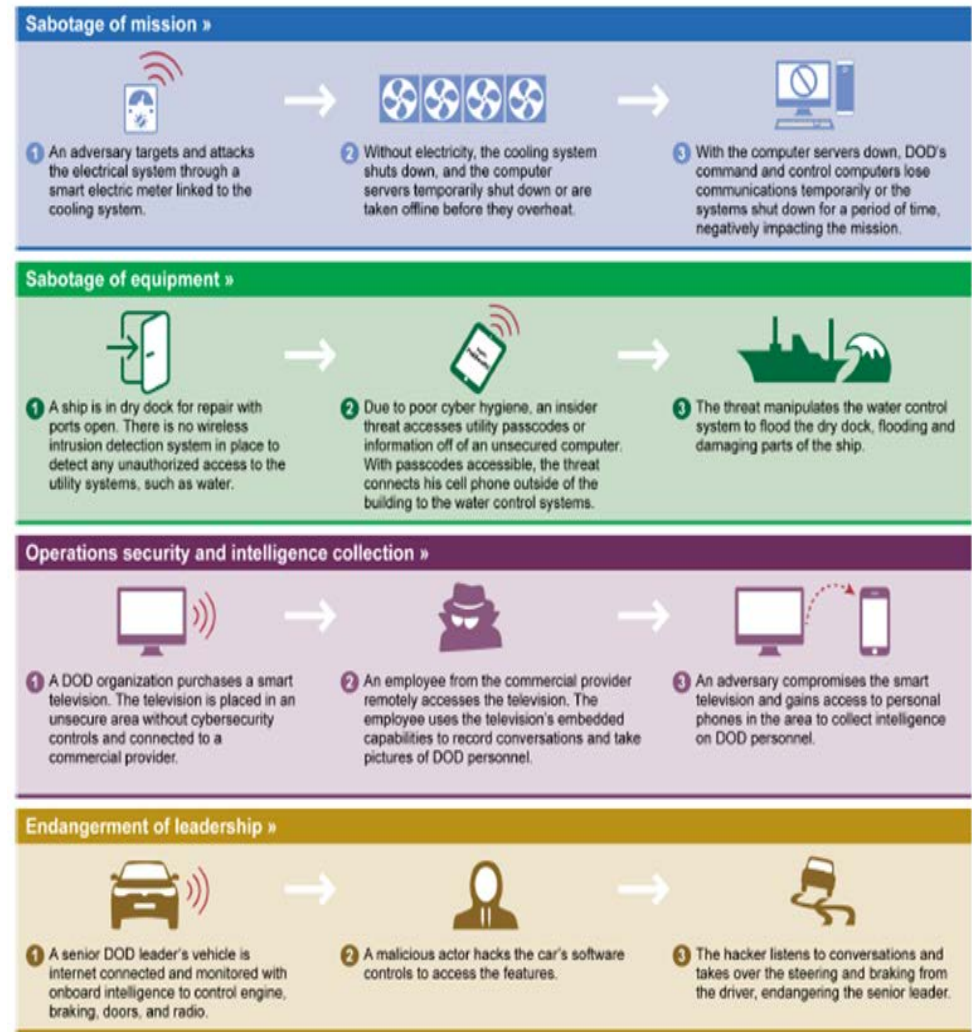
- TV pipeline to devices
- Surveil & steal critical data

Leadership Targets

- Hijack Pentagon leader's car
- Steer car over the cliff

[GAO-17-668]

Figure 2: Notional Internet of Things (IoT) Scenarios Identified by Department of Defense (DOD)



IoT Cyber Threats & Risks

Who Regulates? And How?





Who Regulates IoT?

Before IoT: Parallel Regulatory Regimes (Privacy & Cyber)

Patchworks

- Privacy
 - HIPAA
 - GLB
 - FERPA
 - Privacy Act
- Cyber
 - FISMA
 - FAR
 - DFARS
 - GSA, HHS



Technology Fusion

- IoT & Drones
 - “next trillion files”
 - FAA regulate IoT?
- IoT + Cloud + AI
 - FedRamp
 - DFARS
 - Antitrust (DOJ vs. FTC)



Who Regulates IoT?

Congressional Oversight on the Hill

Congressional Committees

- “more than 30 different congressional committees” *Politico* (2015)

Legislative Actions

- Sen. Resolution 110 (2015)
- S.88 - Developing Innovation & Growing the Internet of Things (DIGIT) Act
- S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017
- H.R.3985 - Internet of Medical Things Resilience Partnership Act of 2017
- H.R. 1324, Securing IoT Act (2017)

Congressional Hearings & Reports

- Sen. Report No. 115-90, (June 5, 2017)
- **Lots & Lots of Senate & House Hearings**





Who Regulates IoT?

Federal Agencies & IoT Oversight

Federal Agencies

- **FCC**
 - Spectrum management
- **DHS**
 - Critical infrastructure
- **FTC**
 - Consumer devices
- **FDA**
 - Medical devices



& More Agencies

- **DOE**
 - Smart grid
- **DOT**
 - Connected cars
- **DOD**
 - Advanced Tech
- **DOJ**
 - Law enforcement

Who Regulates IoT?

Federal & State Enforcement Actions



Criminal Enforcement (DOJ)

- Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant DDoS Attacks: Defendants Responsible for Creating “Mirai” and Clickfraud Botnets, Infecting Hundreds of Thousands of IoT Devices with Malicious Software (Dec. 13, 2017) [DOJ Press Release]

Administrative Enforcement (FTC)

- Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children’s Privacy Law and the FTC Act: Settlement marks the agency’s first children’s privacy and security case involving connected toys (Jan. 18, 2018) [FTC Press Release]

State Enforcement

- In Safetech IoT Settlement, New York Attorney General Outlines Reasonable Security Program, iptechblog (June 1, 2017) [NY AG Settlement]

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



IoT Cyber Threats & Risks

What Standards? And Where?



What are the IoT Cyber Standards?

Department of Homeland Security Guidance

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



1. Incorporate Security at the Design Phase
2. Advance Security Updates and Vulnerability Management
3. Build on Proven Security Practices
4. Prioritize Security Measures According to Potential Impact
5. Promote Transparency across IoT
6. Connect Carefully and Deliberately

U.S. Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0
November 15, 2016

What are the IoT Cyber Standards?

Food & Drug Administration – Medical Devices

Varying Security Regimes – Patient Risk

- Pre-Market Considerations
- Post-Market Considerations



NIST Cybersecurity Framework

- 2014 NIST Framework
- Identify, Protect, Detect, Respond, & Recover

Elements for Post-Market Cyber Program

- Identify: maintain safety & ID market data (e.g., complaints & returns)
- Protect/Detect: assess & detect vulnerabilities, risks & threats
- Protect/Respond/Recover: assess security controls
- Mitigate:
 - Assess & mitigate **safety** risks
 - Preserve essential **performance** (i.e., efficacy)

“Contains Nonbinding Recommendations”

Contains Nonbinding Recommendations

Postmarket Management of
Cybersecurity in Medical Devices

Guidance for Industry and Food and
Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.



U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

What are the IoT Cyber Standards?

Department of Defense – Networks & Military Technology

DIVING INTO UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



GAO Assessments

- House Report 114-537 (2017 NDAA): assess DOD
- House Report 114-573 (2017 IAA): assess Intelligence agencies

DOD & Intelligence Assessments

- Multiple DOD/IC Assessments: Defense Science Board, DOD CIO Report, Joint Staff, DNI Threat Assessment


“DOD has stated that it is entering a rapidly deepening pool of vulnerability.”



No Unified IoT Oversight or Standards

- “According to DOD officials, no one specific office or entity is responsible for IoT security.”
- “DOD has policies and guidance for IoT devices, but gaps remain.”

United States Government Accountability Office



Report to Congressional Committees

July 2017

INTERNET OF THINGS

Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD

What are the IoT Cyber Standards?














Department of Defense – Networks & Military Technology

DIVING INTO UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Figure 3: Examples of Department of Defense (DOD) Policies and Guidance on Types of Internet of Things (IoT) Devices^b

Policy and guidance	Sponsor	Ownership of device	Type of device
<i>Introduction and Use of Wearable Fitness Devices and Headphones within DOD Accredited Spaces and Facilities</i> April 2016	DOD Chief Information Officer	 Personal	 Fitness devices
DODI 8420.01, <i>Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies</i> November 2009	DOD Chief Information Officer	  Government Personal	 Smart watches and other portable electronic devices
Component Policies on Wireless and Personal Portable Electronic Devices 2014 and 2016	DIA, DISA, and Department of the Navy		
Security Technical Implementation Guides for specific DOD-issued mobile devices like Apple and Blackberry 2016	DISA	 Government	 Smartphones
<i>Unified Facilities Criteria: Cybersecurity of Facility-Related Control Systems</i> September 2016	OSD and Departments of the Army, Navy, and Air Force	  Government Vendor*	 Infrastructure devices
<i>Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) for Department of Defense (DOD) Industrial Control Systems (ICS)</i> January 2016	U.S. Cyber Command and OSD	  Government Vendor*	 Infrastructure devices

DIA Defense Intelligence Agency
 DISA Defense Information Systems Agency
 DOD Department of Defense
 OSD Office of the Secretary of Defense

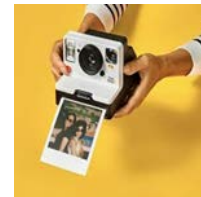
Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-668

What are the IoT Cyber Standards?

National Institute of Standards & Technology (NIST)

NISTIR 8200

- Purpose: survey existing IoT cyber standards



Multiplicity of Standards

- Relevant NIST standards (**over 70**)
- Agency guidance (e.g., DOT ITS-JPO, FDA, GSA)
- Existing & emerging industry standards (e.g., ISO/IEC, OMG)



Key Findings & Non-Findings

- IoT Definition: None
- Functional Applications: Connected vehicles, consumer devices, healthcare/medical devices, smart buildings & smart manufacturing
- Cyber Standard: No one-size-fits-all
- Core Areas: 11 core areas for cybersecurity standardization

Draft NISTIR 8200

Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)

Prepared by the Interagency International Cybersecurity Standardization Working Group.



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

What are the IoT Cyber Standards?

NISTIR 8200: Status of Cybersecurity Standardization for Several IoT Applications

Table 4 – Status of Cybersecurity Standardization for Several IoT Applications

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Cryptographic Techniques	ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C	Standards Available Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake
Cyber Incident Management	ETSI ; ISO/IEC JTC 1; ITU-T; PCI	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
Identity and Access Management	ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C	Standards Available Slow Uptake	Standards Available Slow Uptake	Some Standards Slow Uptake	Standards Available Slow Uptake	Standards Available Slow Uptake

What are the IoT Cyber Standards?

NISTIR 8200: Status of Cybersecurity Standardization for Several IoT Applications



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Information Security Management Systems	ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake	Some Standards Slow Uptake
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group; UL	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented	Standards Needed Not Implemented
Hardware Assurance	ISO/IEC JTC 1; SAE International	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Slow Uptake	Some Standards Not Implemented	Some Standards Not Implemented

IoT Cyber Threats & Risks

Protecting Yourself on the IoT Frontier

Define IoT

- Enforceable contract terms or security plans?

Tailor your requirements

- No one-size-fits-all (per NIST) – vs. sector-by-sector

Pick your security standard

- NIST Framework? NIST 800-171?
ISO? OMG?

Perform your risk assessment

- All standards – Bang-for-buck

Know your supply chain

- Market leverage & privity?
- Security savvy?

Wild, Wild West of IoT



Who Regulates IoT?

Regulating the Undefined

NIST Publication

“However, the current Internet of Things (IoT) landscape presents itself as a mix of jargon, consumer products, and unrealistic predictions. There is **no formal, analytic**, or even descriptive set of the **building blocks** that govern the operation, trustworthiness, and lifecycle of IoT. This **vacuum between the hype and the science, if a science exists**, is evident. Therefore, a composability model and vocabulary that defines principles common to most, if not all networks of things, is needed to address the question: “**what is the science, if any, underlying IoT?**”

[NIST, Draft NISTIR 8063 (Feb. 2016)]

Privacy of Things

“The Internet of Things (IoT) will create the single largest, **most chaotic conversation in the history** of language. Imagine every human being on the planet stepping outside and **yelling at the top of their lungs everything that comes into their heads**, and you still wouldn’t be close to the scale of communications that are going to occur when all those IoT devices really get chattering.”

[Geoff Webb, *How will billions of devices impact the Privacy of Things?* (Dec. 7, 2015)]

Navigating “Ordinary” Information Security & Privacy Risk

Legal Principles, Information Sharing, and Incident Preparation/Response



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Managing Ordinary and Government Contract Risk Throughout the Business Lifecycle

- Governance
- Corporate policies and procedures, especially Incident Response Plan
- Vendor management, compliance terms, and flowdown
- Business transactions and privacy and information security due diligence
- Training and awareness



Managing Risk with Effective Incident Response: Prepare, Practice, and Execute

- Legal Principles:
 - Minimizing attack surface – e.g. does IoT need to be connected to myriad of devices or does a single ISP suffice?
 - Spreading risk – not one person owns all the risk
- Incident response plan (IRP)
- Incident response team (IRT), including third party forensics and outside counsel
 - IRT considered a “team sport”
 - Information Technology, Legal, Business, Communications, CEO
- Tabletop exercises

Incident Response

- Focus on IT attacks and prevention
 - Offensive and defensive perspectives
- Incident Response Plan (IRP)
 - Manage external risks
- Investigation triggered by incident report -- Focus on security, mitigation and evidence gathering
- Data breach-related notification requirements
 - Legal, regulatory and contractual compliance
 - Response timelines
 - Methods of notification
- Anticipate and assess litigation risks



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Incident Preparation

- Tabletop Exercises
 - Conduct tabletop exercises at multiple levels
 - Ground level/first responders
 - Executive level
 - Enterprise level: don't overlook middle management
- Vulnerability Assessments
- Pen Tests
- Train to Incident Response Plan:
 - Write to IRP, Train to IRP, Review IRP

Cyber Insurance Coverage

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

- Cyber insurance encompasses both third-party losses (liability to others) and first-party losses (losses to policyholder's own business interests).
- Cyber coverage programs are often negotiated based on individual company needs, especially for larger insureds.
- No "standardized" insurance policy forms, so various insurers' and brokers' policy forms differ in the scope of coverage provided.
- Type of losses cyber insurance may include:
 - Privacy & Network Security Risk
 - Privacy & Network Security Liability
 - Privacy Regulatory Fines and Penalties
 - Media Liability
 - Dependent Business Interruption/Dependent System Failure
 - Cyber Extortion
 - Digital Asset Restoration
 - PCI Fines and Penalties
 - Breach Event Expenses
 - Network Business Interruption
 - System Failure

Post-Dive Wrap-Up: Managing Information Security & Privacy Risk

- Identify and Classify Data and Systems (CUI? Classified? PII? Regulated?)
- Implement Physical, Technical, and Administrative Controls to address risks, compliance and otherwise
- Establish Appropriate Governance
- Review and Update Policies & Procedures Regularly
- Evaluate Whether Public-Facing Statements on Security and Privacy Match Current Practices
- Analyze Internet of Things interconnections
- Prepare for Data Incidents in Advance (Incident Response Plan, Team, Tabletop, Data Breach Toolkit)
- Review Vendor Management Process
- Analyze Audit and Reporting Processes
- Participate in Industry and Government Partnerships

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

David Bodenheimer

(202) 624-2713

dbodenheimer@crowell.com

Michael Gruden

(202) 624-2545

mgruden@crowell.com

Paul Rosen

(213) 443-5577

prosen@crowell.com

Evan Wolff

(202) 624-2615

ewolff@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Ethics and Compliance in a Consolidating Market

David Robbins

Rachel Fleischer, Anthem, Inc.

Sean Hoffman, KPMG LLP

Laura Baker

Stephanie Crawford

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Topics to be Covered

- 1) Updates on Issues of Ethics & Compliance (20 min)
- 2) Questions & Answers with Panel (30 min)

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Updates on Issues of Ethics & Compliance

Suspension & Debarment

- Trends in Fiscal Year 2017 & What to Expect in 2018

	Total Exclusions	Firms	Individuals	Special Entities
FY 2016 SAM Data	2,229	284	1,738	207
FY 2017 SAM Data	1,878	262	1,415	201
Change	(351)	(22)	(323)	(6)

- New SAM Registration Requirements After Fraudulent Activity

DOJ Guidance on Compliance

Evaluation of Corporate Compliance Programs

(Feb. 2017)

- Provides a list of compliance-focused topics and questions DOJ believes are relevant to its evaluation of corporate compliance programs.
- DOJ will take into account whether companies:
 - (i) have adequate compliance programs;
 - (ii) cooperate and self-disclose any wrongdoing; and
 - (iii) take suitable steps to remediate problems.

New FCPA Corporate Enforcement Policy

(Nov. 2017)

- To increase the volume of voluntary disclosures from corporations.
- To enhance DOJ's ability to identify and punish culpable individuals.
- A company must implement "an effective compliance and ethics program."

OFCCP Developments

- OFCCP Issues Notices in Advance of Annual Compliance Review
 - no more than 10 establishments of an individual contractor will be on the scheduling list, and
 - no more than four establishments of an individual contractor will be audited by a particular district office.
 - no establishment with a review closed in the last five years will be scheduled for a compliance review this year, an increase from the previous two-year reprieve.
- OFCCP Issues Directive 2018-01
 - Requires OFCCP to adopt a uniform approach to Predetermination Notices in compliance evaluations.
 - OFCCP is now required to:
 - inform the contractor of the agency’s preliminary findings of employment discrimination; and
 - provide the contractor with 15 days to rebut OFCCP’s preliminary findings.

FAR Council Semi-Regulatory Agenda

- Violation of Arms Controls Treaties or Agreements
 - Certify no activity that contributes to determination that a country is not in compliance with arms control, nonproliferation, or disarmament agreements
- Whistleblower Protection for Contractor Employees
 - Make permanent
 - Apply legal fees prohibition to subcontractors

FAR Council Semi-Regulatory Agenda (cont'd)

- Breaches of Personally Identifiable Information
 - Contract terms for PII breaches when a contractor has access to or maintains PII on behalf of an agency
- Controlled Unclassified Information (CUI)
 - Implements NARA CUI program for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI

FY2018 NDAA

- § 889 Report on Defense Contracting Fraud
 - Report of DoD contracts in previous 5 years with contractors with fraud connection
 - Recommendations on penalizing contractors
- § 1045 Prohibition on Lobbying Activities
 - 2-year preclusion (O-9 officers/SES Tier III and above); 1-year preclusion (O-7 and O-8 officers/SES Tier I and II)
 - Banning behind the scenes work intended for use in contact and coordination with lobbying activities of others

Other Developments

- DoD OIG Missile Defense Agency Contractors
 - Failed to properly protect classified information
- DFARS Sources of Electronic Parts Amendment
 - Review when identifying a contractor-approved supplier of electronic parts
- DFARS Promoting Voluntary Post-Award Disclosure of Defective Pricing
 - CO discretion to request limited-scope or full-scope audit

State and Local

- Increased emphasis on vendor responsibility/front end compliance
- In some instances, new disclosures and certifications came into existence:
 - Port Authority New Ethics Code for Vendors
 - Requires vendors to certify compliance
 - Port Authority also implementing past performance evaluations for all construction projects



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Discussion Topics

- Key trends keeping experts up at night
- Ethics/compliance as a valuable asset
 - importance of culture/ethics/compliance in vetting corporate transactions in the consolidating marketplace



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Discussion Topics - continued

- How do you train your workforce about the differences in expectations when dealing with public customers (governments) as opposed to private customers?
- How can you reinforce training so the learning isn't lost?

Discussion Topics - continued

- Scope creep as an ethical issue – when giving more at no cost creates problems



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Laura Baker

(202) 624-2581

lbaker@crowell.com

Stephanie Crawford

(202) 624-2811

scrawford@crowell.com

David Robbins

(202) 624-2627

[drobbins@crowell.com](mailto:d Robbins@crowell.com)

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Small Business Status, Investigations, and Consequences

Steve Byers

Jared Engelking

Olivia Lynch

Amy O'Sullivan



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Agenda

- An environment ripe for fraud and abuse
- Key sources of small business regulatory missteps
- Common schemes and red flag indicators
- Enforcement tools and trends
- The wide net of consequences for entities and individuals
- Illustrative case examples

An Environment Ripe for Fraud and Abuse

- SB status necessary (or beneficial) to access prime and subcontracts (\$100B in prime contracts alone for FY16)
- Complex regulatory overlay applicable to inexperienced contractors
- Fewer checks and balances
 - Control by one or a few individuals
 - Limited or no investment on compliance
 - Pressure from investors, customers, large businesses
 - Heightened diligence needed by teaming partners and buyers

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Key Regulatory Missteps

- Size status requires self certifications
- Dramatic industry variations on “small” based on NAICS Code:
 - Number of employees (100 to 1,500); or
 - Average annual receipts (\$750K to \$38.5M)
- Size accounts for employees/receipts of business and all “affiliates”
 - Centered around concept of control
 - “Totality of the circumstances” analysis that is highly fact intensive
 - Date-specific determinations

Key Regulatory Missteps - Affiliation

Misunderstanding/Misrepresenting “Control”:

- Control refers to ability to control and may be affirmative or negative
- Red flags on quorums or supermajority/unanimous voting requirements
- Control due to terms associated with loans/bonding or “side agreements”

Affiliation Based on “Identity of Interest”:

- Economic dependence based on contractual or other interests
- All/most subcontracts from one entity
- Financial arrangements (loans, bonding, etc.)

Key Regulatory Missteps - Status

Missteps Impacting Status:

- Do the necessary individuals manage the company, control day-to-day operations and long-term decision-making?
- Does the President/CEO have managerial experience of the extent and complexity needed to run the company?
- Do the necessary individuals “directly” and “unconditionally” own at least 51% of the company?

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Key Regulatory Missteps - Workshare

Limitations on subcontracting – SB prime

- Currently two sets of calculations (FAR and SBA regulations) and limits vary based on type of work
- Period for compliance – base period and each individual option period

Added complexity to DOT DBE Program – SB sub

- DBE must perform “commercially useful function”
- Count only value of work performed by DBE
- Additional specific requirements based on type of subcontract

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Common Schemes/Red Flag Indicators

- Straw owners who sell their status
- Pass-through fraud
- Affiliation with larger companies
- Companies that recently outgrew small size status
- Misrepresentations regarding economic disadvantage, etc.
- Inexperienced owner/business dependent on another

Enforcement Tools and Trends

- Enhanced sanctions and penalties
 - Presumption of loss (15 U.S.C. § 632(w)(1); 13 C.F.R. § 121.108(a))
 - Liquidated damages (FAR 52.219-16)
 - SBA Program Fraud and Civil Remedies Act, 31 U.S.C. §§ 3801-12
- Size protests
 - Elimination from competition
 - Can serve as start of investigation
- False Claims Act
- Criminal Prosecution
- Suspension & Debarment

Wide Net of Consequences

Investigations and cases reflect harsh consequences for multiple companies and individuals

- Large businesses involved tend to get the media spotlight (*i.e.*, GTSI)
- Multiple named defendants with varying roles in the scheme
 - Central bad actors typically have familiarity with SBA requirements
 - Increases complexity of scheme due to measures to avoid detection
- False Claims Act liability sought for large businesses through increasingly attenuated connections (deep pockets)
- Disproportionately large percentage of entities suspended or debarred are small businesses (well over 50% for most agencies)

Recent Cases

U.S. ex rel. Savage (E.D.Wa. 2017)

- Large prime contractor, accused of misrepresenting status of small businesses to meet small business subcontracting plan goals
- Lost motion for partial summary judgment on damages
- Court found that under "presumption of loss" rule damages should be based on the **full value** of the improperly awarded subcontracts.

Recent Cases

U.S. ex rel. Scollick (D.D.C. 2017)

- Motion to dismiss denied where surety bond issuers allegedly caused presentment of false claims by bogus SDVOSBs where:
 - Proposals were dependent upon the issuance of surety bonds; and
 - Issuers allegedly knew their clients were shell companies

Recent Cases

ADS, Inc. (2017)

- \$16 million FCA settlement by large prime accused of "conspiring with and causing purported small businesses to submit false claims . . ." due to undisclosed affiliation
- Scheme involved different affiliates
- Ranks as one of the largest recoveries involving alleged fraud in connection with small business contracting eligibility
- "OIG will aggressively pursue companies that, through false statements, wrongfully benefit from small business set-aside contracts."

Recent Cases

U.S. ex rel. Cherwenka (D. Minn. 2018)

- Relator alleged that large primes knew a subcontractor supply distributor did not qualify as small because it was affiliated with its large supplier
- But SBA had investigated and blessed that relationship through an approved mentor-protégé agreement
- Defendants won motion to dismiss
- Mentor-protégé program, if utilized properly, can be a vehicle to provide support between companies free from consequences of affiliation

Recent Cases

U.S. v. Dial (D. Kansas 2018)

- Criminal prosecution of service-disabled veteran "who received payments in exchange for use of his name, signature and veteran status in order to make his role in the business appear legitimate, while doing little actual work" on \$40 million worth of DOD contracts
- Company was instead run by "Person A" and Dial was rarely even present in the office

Headliner Cases

GTSI Corp. (2010)

- Large contractor that had grown from small suspended by SBA for participating in a classic pass-through scheme under which GTSI would receive virtually all of the revenue on set-aside contracts
- CEO and GC removed and independent monitor imposed as part of administrative agreement

MicroTechnologies, LLC (2014)

- MicroTech and its CEO suspended due to affiliation with two other entities through common investors and related misrepresentations when applying for 8(a) status
- Suspension lifted (1) for MicroTech after CEO relinquished control during investigation and (2) for CEO after ethics and compliance training and sit-out period from management

DBE Fraud Cases March On

- DBE cases represent around 30% of DOT OIG active procurement and grant fraud investigations
- *United States v. Nagle*, 09-CR-00384-001, (M.D.PA July 26, 2013)
 - Co-owners of Schuylkill Products, Inc. set up sham company (Marikina) – 15 year scheme involved over \$130M in contracts (largest DBE fraud scheme in history)
 - Sham owner paid small fee but SPI employees performed all work and covered up SPI name on equipment
 - Co-owners served jail time and fined; other SPI executives and Marika owners sentenced to prison and ordered to pay restitution

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Stephen Byers

(202) 624-2878

sbyers@crowell.com

Jared Engelking

(202) 624-2815

jengelking@crowell.com

Olivia Lynch

(202) 624-2654

olynch@crowell.com

Amy O'Sullivan

(202) 624-2563

aosullivan@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Off-Limits Information and Employee Mobility

Peter Eyre

Trina Barlow

Valerie Goo

Yuan Zhou

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Agenda

- Common Scenarios
- Legal Considerations
- Reacting to Suspected Receipt of Off-Limits Information
- Best Practices for Preventing and Deterring Receipt of Off-Limits Information

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Common Scenarios

- Employee mobility
- Hiring former government employees
- Inadvertently sent documents
- Deliberately obtained off-limits information
- Competitive intelligence

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Legal Considerations

Trade Secrets

- Definition: Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
 - (1) derives independent economic value from not being generally known to the public; and
 - (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy

80% of trade secret loss from employees, contractors, and trusted insiders

- Departing or disgruntled employees
- Intentional (malicious)
- Inevitable (knowledge acquired)
- By ignorance

Trade Secrets

Broad Scope of Trade Secrets

- Customer Lists
- Training Materials, Programs, and Methodology
- Pricing and Cost Data
- Strategic Plans and Forecasts
- Competitive Analyses and Intelligence
- Mechanical and Physical Processes
- Blueprints, Designs, and Prototypes
- Algorithms and Formulas
- Software and Source Code

Trade Secrets Spectrum

Tell No One Share with Confidentiality Publication



Perfect
Secrecy

No
Secrecy

“Secrecy Continuum”

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Defend Trade Secrets Act

- Near unanimous support in both houses of Congress
- Signed into law May 11, 2016
- What's changed?

Unchanged

- Definition of trade secrets
- Definition of misappropriation
- All UTSA remedies still available
- Statute of limitations

New

- Jurisdiction
- Whistleblower provision
- Ex parte seizure
- International provisions
- Sealing provision

Defend Trade Secrets Act

- Whistleblower Protection: Immunity from criminal or civil liability under state or federal law for disclosure of trade secret:
 - If made in confidence to federal, state or local official solely for purpose of reporting or investigating suspected violation of law
 - If disclosed in complaint or other document filed in lawsuit or other proceeding if made under seal
- Notice of immunity required in any contract (after May 2016) or agreement with employee (includes contractors and consultants)



Defend Trade Secrets Act

- Ex Parte Seizure
- “Extraordinary” additional remedy
 - Applicant must meet specific (and burdensome) requirements
 - Court must follow very specific procedure
 - Fees and/or damages allowed if remedy is unwarranted



Contractual Confidentiality Obligations

- Non-competes
 - Historically enforceable where narrowly tailored
 - But, non-competes increasingly disfavored by courts (concerns about job insecurity and employee mobility)
 - Executive Order 13495
- Non-solicits
- Confidentiality/nondisclosure
- Continuity of services
 - Relevant FAR clauses
- Contract clauses and teaming agreements

Off-Limits Procurement Information

- Implications of private disputes v. government overlay
- The government must establish a level playing field
- This includes making sure that:
 - (1) companies do not obtain an unauthorized competitive advantage by virtue of receiving non-public information; and
 - (2) Government decision making is free from the appearance of impropriety
- Exchanging or obtaining certain types of procurement information may:
 - Expose employees and the company to liability
 - Have bid protest implications
 - Result in exclusion from the competition
 - “Appearance of impropriety” may be sufficient to sustain protest

Procurement Integrity Act

- Prohibitions on knowingly disclosing and obtaining contractor bid or proposal or source selection information:
 - Subsection 2102(a):
 - Disclosure prohibition
 - Applicable to current or former government officials and certain acquisition support contractors/consultants
 - Subsection 2102(b):
 - “Obtaining” prohibition (term undefined)
 - Applicable to “a person” (term interpreted by caselaw)

Procurement Integrity Act

- Covered information is inclusive of some trade secrets
- **“Contractor bid or proposal information”** means the following if submitted to a Federal agency as part of, or in connection with, a bid or proposal to enter into a Federal agency procurement contract, if that information previously has not been made available to the public or disclosed publicly:
 - Cost or pricing data
 - Indirect costs and direct labor rates
 - Proprietary information about manufacturing processes, operations, or techniques marked by the contractor
 - Information marked as “contractor bid or proposal information”

Procurement Integrity Act

- **“Source selection information”** means information prepared for use by a Federal agency to evaluate a bid or proposal to enter into a Federal agency procurement contract, if that information previously has not been made available to the public or disclosed publicly
 - Source Selection and Evaluation Plans
 - Proposed costs or prices submitted in response to a Federal agency solicitation
 - Cost/Price and Technical Evaluation reports
 - Independent Government Cost Estimates
 - Competitive range determinations
 - Rankings of bids, proposals, or competitors
 - Catch all: anything else marked “Source Selection Information”

Procurement Integrity Act

- PIA obligations exist until contract award
- Requires government nexus
- The Savings Provision (41 U.S.C. § 2107):
 - The PIA does NOT restrict a contractor from disclosing its own bid or proposal information or the recipient from receiving that information
- Presents challenges with information provided to employees, teaming partners, consultants, etc.

Procurement Integrity Act

- Requirement for Prompt Reporting of Potential PIA Violations (41 U.S.C. § 2106)
 - No protest alleging a PIA violation unless the person, **no later than 14 days after the person first discovered the possible violation**, reported to the agency responsible for the procurement the evidence of the offense
 - Protests are only ripe when the agency completes its investigation after the 14-day notice has been made
 - Must file challenge at GAO within 10 days of notice unfavorable investigation outcome. *See SRS Techs.*, B-277366, July 30, 1997, 97-2 CPD ¶ 42

Organizational Conflicts of Interest

- FAR Definition (FAR 2.101): “An OCI arises when, because of other relationships or circumstances, a contractor may be unable, or potentially unable, to render impartial advice or assistance to the government, the contractor’s objectivity in performing the contract work is or might be impaired, and/or the contractor would have an unfair competitive advantage”
- Three types:
 - A “biased ground rules” OCI has been found where one offeror provides assistance in drafting the RFP, SOW, or specifications (i.e., set ground rules for another gov’t contract)
 - Impaired objectivity if a contractor is in the position of evaluating its own performance or products, or the performance or products of a competitor.
 - Unequal access to information that the contractor was fully entitled to access.
- Potentially result in disqualification or can prevent contractor from pursuing future work

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Unfair Competitive Advantage

- The government must maintain a level playing field and avoid any appearance of impropriety
- Disqualification is potential risk if one offeror receives information that is competitively useful but not available to all offerors
- Particular risk for former government employees; notable GAO case law

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Reacting to Suspected Receipt of Off-Limits Information

Reacting to Suspected Receipt of Off-Limits Information

- Preparation and planning (Code of Conduct)
- Training
 - Know what to look out for
 - Form of information (not necessarily written)
 - Types of markings (e.g., “proprietary,” “source selection sensitive”)
 - Educate employees on what to do
- IT/Vendors
 - Document retention & forensic analysis
 - Computer use restrictions – CFAA (tool to protect competitively sensitive data)
 - Private right of action against person
 - Who knowingly and with intent to defraud
 - Accesses a protected computer without authorization, or exceeds authorized access
 - Underscores need to maintain computer use policy restricting employees’ authorized access to and use of company computers

Reacting to Suspected Receipt of Off-Limits Information

- Immediate steps
 - Quarantine the off-limits information
 - Conduct forensic analysis of the off-limits information (e.g., receipt date, access, other metadata)
 - Investigation of source of off-limits information
- Longer-term steps
 - Assess use of off-limits information
 - Assess public availability of such information
- Disclosures
 - To potential third parties
 - To Government
- Lessons and common pitfalls

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Best Practices for Preventing and Deterring Receipt of Off- Limits Information



Best Practices for Preventing and Deterring Receipt of Off-Limits Information

On-boarding

- Determine protection strategy
 - Which employees will sign which agreements?
 - What are you trying to protect?
 - How are you trying to protect it?
 - Establish a repeatable process with HR
- Training: Educate employees about what constitutes trade secrets and protected off-limits information
 - Provide clear definitions of what is protected
 - Reinforce education and company commitment to safeguarding trade secrets/impropriety of off-limits information
 - Reflected in policies & procedures

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

On-boarding

- Validation and controls
- Requesting and reviewing any pre-existing non-competes or non-solicits a new recruit may have
- Getting a certification that employee is not violating a non-compete or improperly using prior employers' information
- Special steps for former government employees
- Be mindful of “presumption of use”

Off-boarding

- Reiterating obligations to departing employees during the off-boarding process
- Conduct exit interview & ask the right questions
- Demand return of everything; verify return of emails, hard drives, portable media and storage

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

Rules of the Road

- Before Proposal Submission
 - Comply with RFP requirements about communications with the Agency
 - Agency “point of contact” – use formal channels only
- After Proposal Submission
 - Generally there should be no attempt to communicate unilaterally with the government after submission of proposals

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Best Practices for Preventing and Deterring Receipt of Off-Limits Information

Rules of the Road

- After Completion of Procurement
 - Some otherwise protected information may be releasable by the government (e.g., FOIA, Post-award debriefings)
 - Government must make this determination through official channels
 - Nonetheless, contractors must remain vigilant even after a procurement for potential risks
- At all times
 - If employees are offered or receive information and are unclear whether they're authorized to receive the information, then (1) immediately contact the Legal Department *before* reviewing the information; and (2) *do not share* the information with anyone else unless they have obtained clearance from the Legal Department (do not print, forward by email, or copy)

Best Practices for Preventing and Deterring Receipt of Off-Limits Information

Internal Controls

- IT controls (e.g., document retention, USB/hardware triggers, monitoring access & audits)
 - Physical security for access to trade secrets
 - Data security protocols
 - » Password protection / reminder pop-ups for employees
 - » Combination of protections for highly valued information
 - » Regularly run security checks to ensure systems have not been compromised and take action if they have
 - » Employee remote access issues
 - » Monitoring devices/software to protect most valuable assets
- Creating a Culture: training & awareness

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



QUESTIONS?

Trina Barlow

(202) 624-2830

tbarlow@crowell.com

Peter Eyre

(202) 624-2807

peyre@crowell.com

Valerie Goo

(213) 443-5505

vgoo@crowell.com

Yuan Zhou

(202) 624-2666

yzhou@crowell.com



Claims and Affirmative Recovery: Keeping the Customer Happy While Watching the Bottom Line

Steve McBrady

Skye Mathieson

Monica Sterling

Sharmi Das

Michelle Coleman

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Overview

- Affirmative Contractor Claims and REAs
- Defending Against Government Claims
- Steps to Take Right Now

Affirmative Recovery

- Identifying Affirmative Recovery Opportunities
- Pursuing Claims Recovery



Affirmative Recovery

- Companies doing business with the U.S. Government may be entitled to affirmative recovery based upon a variety of legal theories.
 - Increased performance costs attributable to Government
 - Costs resulting from Government-initiated contract termination
 - Costs arising from Government-caused delay
 - Costs arising from differing site conditions
 - Unpaid costs under money-mandating statutes
 - Costs of remediating certain environmental pollution and toxic tort litigation costs
 - Indemnification for certain hazardous activities
- What they all share in common: the Government does not pay claims unless they are asserted, pursued, and appropriately documented.



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Changes

- Express or constructive
- Importance of defining terms during contract negotiation
 - *Family Entertainment Servs.*, ASBCA No. 61157, Oct. 24, 2017.
- Impact of limited funding
 - “Scope creep”
 - Increased use of termination for convenience (and importance of addressing contract changes promptly during performance)
- Impact of failure to provide timely notice
 - *K-Con Bldg. Sys., Inc. v. United States*, 778 F.3d 1000 (Fed. Cir. 2015).
- Value of timely claim to securing advantageous settlement

Deductive Changes

- Deductive change (“de-scope” by deleting work). Permissible if “in the general scope of the contract”
 - Similar to a partial Termination for Convenience.
- Produces a *downward* equitable adjustment to the extent of the savings to the contractor due to the deletion
 - Generally priced based on how much the deleted work “would have cost” (or “anticipated cost” approach)
 - But if the de-scoped work is “severable” (e.g., FFP CLIN), then boards typically use an “as-bid” approach (similar to T4C methodology)
 - Government has burden to prove its entitlement to an equitable adjustment under either methodology
- Considerations:
 - Would the deleted work have been profitable?
 - Potential downstream performance impacts of the work deleted (e.g., subcontract pricing and supplier chain complications)

Differing Site Conditions

- When the conditions at a particular site are different from what was expected.
- Two types: (1) conditions encountered are different than RFP; or (2) conditions encountered are different than industry would typically expect.
- Applies to Construction and Non-Construction (e.g., latent condition encountered during installation, maintenance, repair)

Commercial Items

- Under Commercial Item clause (FAR 52.212-4), all changes must be agreed bilaterally.
 - But if the CO issues a **unilateral** direction / change order, must the Contractor perform the change?
 - Is it a Government **breach**?
- How should the equitable adjustment to perform the change be measured?
 - As **actual costs + profit** (standard) **or** something else?
- *ULS*, ASBCA No. 56850, June 2016.
 - Commercial item contract for satellite launch services. FFP prices per launch vehicle (CLINs by size/weight)
 - Government ordered a “small” (cheaper) rocket.
 - CO’s constructive changes made payload weight grow to need a “medium” rocket.
 - ULS didn’t reject the constructive change. Chose to launch with medium rocket (for safety).
 - Gov’t wants to pay for the actual cost impact of launching the medium (~\$60M). ULS wants to re-price all FFP CLINs (~\$400M).

Government Delays

- FAR 52.242-17 provides a broad remedy for “any” CO action “or inaction” that affects performance and causes cost or schedule impacts
 - Submit timely notification of delay(s) to CO (at least CC’d)
 - Ensure your potential delay claim is not released through contract modification
 - No profit for -17 delays
- Stop Work Order:
 - Can be issued for 90 days (or more by agreement).
 - When the period ends, the contractor must resume or the CO must terminate the work.
 - Contractor entitled to equitable adjustment remedy + profit (FAR 52.242-15)

Termination for Convenience

- Unilateral termination without stated reason
- Generally entitles contractors to costs and losses incurred
- FAR cost principles and case law can inform extent of negotiated settlement (including commercial item contracts, *SWR, Inc.*, ASBCA No. 56708, Dec. 2014)
 - Loss of useful value
 - Initial costs
 - Subcontractor claims
 - Costs preceding Notice to Proceed (*Pro-Built Const. Firm*, ASBCA No. 59278, June 1, 2017)

Termination for Convenience

- Efforts to restrict agency funding
- Limitation of Cost/Funding provisions
 - require contractor notice where funds are running out and put the risk of continued performance on the contractor
 - Relieves the Government of liability for “costs incurred in excess of” allotted funding “[e]xcept as required by other provisions of this contract, specifically citing and stated to be an exception to this clause”
- Uncertain funding for negotiated equitable adjustments
- Greater emphasis on the need to address contract changes promptly during performance

Termination for Convenience

- Hypo: Under a contract to manage soldiers' vehicles in Hawaii, the Government issued a stop-work order and then T4C'd, but CO refused to reimburse costs that post-date termination.
- Result: \$123,489.37 plus CDA interest awarded because contractors are entitled to "fair compensation" with reference to FAR 31 cost principles. *SWR, Inc.*, ASBCA No. 56708, Dec. 2014.

Breach as Recovery

- Government's inadequate preparation of estimates in solicitation
 - *Agility v. United States* (Feb. 2017, Federal Circuit)
- Government duty of good faith and fair dealing
 - Affirmative duty to cooperate
 - Negative duty not to hinder
- Improper T4C allows recovery of breach damages
 - Old and new cases show this is still a viable allegation
- What appears to be a small breach can lead to big damages
- Sword vs. Shield: Use breach as both offensive avenue for recovery and defensively to shield company from Govt's allegations of breach/noncompliance.
 - Prior Material Breach Doctrine: *Laguna Constr. Co. v. Carter*, 828 F.3d 1364 (Fed. Cir. 2016)

Statute of Limitations

- Claims must be submitted “within 6 years after the accrual of a claim.” (CDA § 7103(a)(4)(A)).
 - SOL is a double-edged sword. Strict enforcement is helpful to bar untimely Govt claims (e.g., cost disallowances, defective pricing).
 - But if your company has an Equitable Adjustment that you are attempting to negotiate with the Govt, the SOL can bar your claim if you aren’t vigilant.
 - Must: (1) ascertain date of “accrual,” and (2) keep an eye on the calendar.
- Ascertaining the moment of “accrual” is tricky and subject to constantly changing case law.
 - *Kellogg Brown & Root Servs., Inc. v. Murphy*, 823 F.3d 622 (Fed. Cir. 2016) (“some injury” vs. “sum certain”)

Statutory Claims

- Recovery under money-mandating statutes
- Company or group(s) of companies to recover money from the U.S. Government in the event of non-payment
- Recent examples:
 - The Affordable Care Act (risk corridors, reinsurance, CSR)
 - The American Recovery and Reinvestment Act

Environmental / Indemnification

- Costs of remediating certain environmental pollution and toxic tort litigation costs
 - Recovery under P.L. 85-804 and 10 U.S.C. § 2354 indemnification clauses
 - Recovery under “Taxes” clauses
 - Recovery under World War II era indemnification clauses
 - In addition to traditional CERCLA actions

Defending Against Govt Claims: 1) Termination for Default

- It can happen!
- Considerations
 - Liquidated damages
 - Reprourement costs
 - SAM record: reputation damage
- Importance of timely appeal
 - *Elham Ahmadi Const. Co.*, ASBCA No. 61031, Sept. 21, 2017

Defending Against Govt Claims:

2) Fraud

- Boards' Jurisdiction is Evolving
- Fraud during **formation** has always been grounds to deny Contractor's claim because the contract is "Void Ab Initio." *International Oil (2018)*
- ASBCA: Govt can now assert "Void Ab Initio" as an affirmative Govt claim (seeking complete forfeiture) based on alleged fraud committed during contract performance (e.g., re-pricing CLINs in a Mod).
 - *Supreme Foodservice* (ASBCA) – Govt claim for \$8.3B forfeiture
 - No need for DOJ to obtain conviction or even pursue charges.
- CBCA: In matter of first impression, Board found that the CO's subjective "suspicion" and referral based on potential fraud vitiated the Board's jurisdiction to accept the appeal (even as a deemed denial). *Savannah River (2017)*.





DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Takeaways

- Impact of uncertain funding
 - Pressure to provide concessions after performance begins
 - Terminations for convenience
 - Delays due to Government constraints
 - Uncertain funding for negotiated equitable adjustments
- Proactive protection of rights under the law **during performance**
- Continuous identification of potential claims
 - Training
 - Timely and adequate documentation
 - Prevention of waiver
 - Prevention of release

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Two Steps to Take Right Now

- **Identify contracts and programs that are either losing money or less financially viable than anticipated**
 - Determine whether underperformance is fully or partially the Government's fault
- **Seek recovery where the Government has not lived up to its end of the bargain**

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



QUESTIONS?

Michelle Coleman

(202) 654-6708

mcoleman@crowell.com

Sharmi Das

(202) 624-2692

sdas@crowell.com

Skye Mathieson

(202) 624-2606

smathieson@crowell.com

Steve McBrady

(202) 624-2547

smcbrady@crowell.com

Monica Sterling

(202) 624-2549

msterling@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



State and Local Practice Overview

David Ginsberg

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



QUESTIONS?

David Ginsberg

(213) 443-5545

dginsberg@crowell.com



If I Ran the Zoo: Is Commercial Item Procurement a New Wild Adventure?

Lorraine Campos

Chris Haile

Rosamond Xiang

Agenda

- DFARS Final Rule on Commercial Items and the new DoD Commercial Item Guidebook
- Updates from FY 2018 NDAA and Section 809 Panel Report
- Transactional Data Rule and other changes to the GSA and VA Federal Supply Schedule Program

DFARS Final Rule

- DFARS Case 2016-D006
- Implements sections of the National Defense Authorization Acts (NDAAs) for FYs 2013, 2016, 2018
 - FY 2013: ref. § 831
 - FY 2016: ref. §§ 851-53, 855-57
 - FY 2018: ref. § 848
- Does *not* implement all changes from FY 2018 NDAA
- Does *not* implement changes from FY 2017 NDAA

DFARS Final Rule

Encouraging and Expanding Commercial Treatment

- Prior DoD commerciality determinations.
- Conversion from commercial to non-commercial procurement of an item.
- Supplies and services provided by “nontraditional defense contractors.”
- IT products / service purchases over the SAT.

DFARS Final Rule

Burdens for commerciality and price-reasonableness determinations

- Prime contractor information.
- Subcontractor information.
- DFARS ‘hierarchy’ of information.
- Access to books and records.

DoD Commercial Item Guidebook

- New editions published in January 2018, following a draft distributed in Feb. 2017
- Published in two parts:
 - Part A: Commercial Item Determination
 - Part B: Commercial Item Pricing

New Rules in the Pipeline: Sources of Change

- NDAA 2018
- Further review of current regulations on commercial items (under Section 849 of NDAA 2018) including:
 - FAR council determinations not to exempt contracts and subcontracts from certain procurement rules;
 - DFARS regulations requiring specific clauses in FAR Part 12 clauses;
 - DFARS regulations to assess all regulations that require a prime to flow-down clauses for COTS items.
- Section 809 Panel: recommendations on reforming laws and regulations concerning commercial items
- Draft bill of 2019 NDAA (H.R. 5515)

New Rules in the Pipeline: Potential Substantive Changes

- Definitions:
 - Commercial items/services
 - COTS
 - Subcontracts
- Flow-downs
- Supply chain management
- E-Commerce Portals

(Re-)Defining Commercial Items: NDAA 2018 Revisions

- Sec. 820-amends to the definition of a **subcontract** to exclude
 - “[A]greements entered into by a contractor for the supply of commodities that are intended for use in the performance of multiple contracts with the Federal Government and other parties and are not identifiable to any particular contract.”.
- Sec. 847 – Revision to Definition of Commercial Item
 - Amends “**nondevelopmental item**” prong of definition

(Re-)Defining Commercial Items: Section 809 Panel Recommendations

- Separate "commercial item" into "commercial services" and "commercial products“;
- Merge definitions of commercial items and commercial off-the-shelf items;
- Establish a uniform definition of "subcontract" and "subcontractor."

(Re-)Defining Commercial Items: Draft 2019 NDAA

- Congress takes note of the Section 809 Panel Recommendations
- Sec. 831 would clarify commercial items as commercial products or commercial services.
- Sec. 832 would create one single definition for “subcontract”



Managing the Supply Chain

- **Section 807 of 2018 NDAA: Process for Enhanced Supply Chain Scrutiny**—mandate for DoD to develop:
 - Tools to support due diligence, business intelligence or otherwise analyze commercial activity
 - Risk profiles of products or services
 - Integration with intelligence sources
 - Periodic review and assessment of software products and services
 - Synchronization of current authorities for making supply chain decision or improved use of S&D officials
 - Coordination with interagency, industrial and international partners to share information
- **Section 809 Panel recommendations:**
 - Establish preference for commercial items within supply chain
 - Limit the reach of flow-downs to lower-tier suppliers
 - Temper exclusionary policies (e.g., suspension and debarment) against lower-tier contractors.

Managing the Supply Chain: Flow-downs—Sec. 809 Panel

- Minimize mandatory flow-downs for commercial item contracts;
- Revise "termination for convenience" clauses for commercial item contracts;
- Revise DFARS provisions on data rights for commercial product.



Flow-downs: Draft 2019 NDAA

- Sec. 833: limit applicability of certain executive orders and DoD regulations to DoD commercial contracts and subcontracts, to remove transactional barriers between DoD and commercial suppliers.

E-Commerce Portal: NDAA 2018

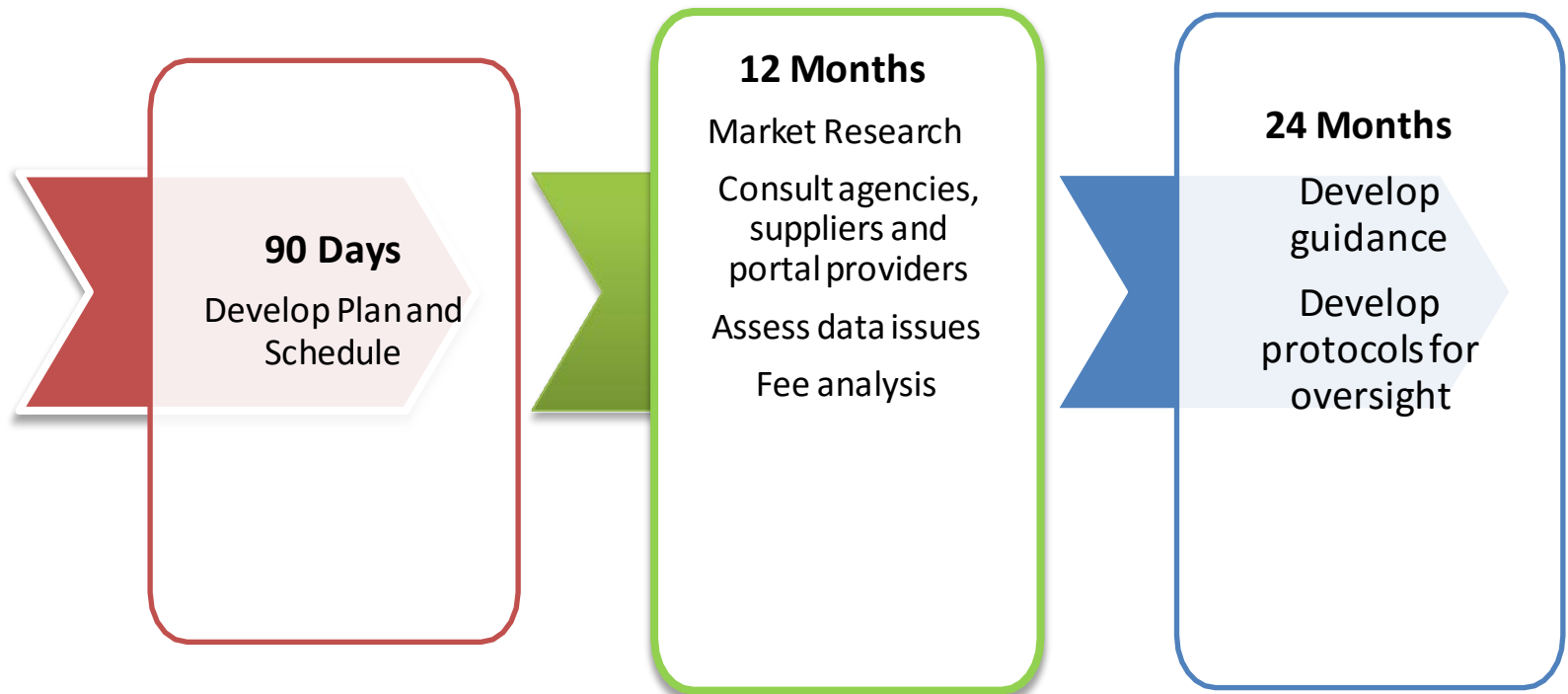
Section 846: Procurement Through Commercial E-Commerce Portals

- Requires a multi-phased program to be established to procure commercial (COTS) products through commercial e- portals to enhance competition, expedite procurement, enable market research and ensure reasonable pricing.
- Procurements from the portal shall be made:
 - to the maximum extent practicable, under the standard terms and conditions of the portal to the maximum extent practicable
 - Under the Simplified Acquisition Threshold

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

E-Commerce Portal: NDAA 2018



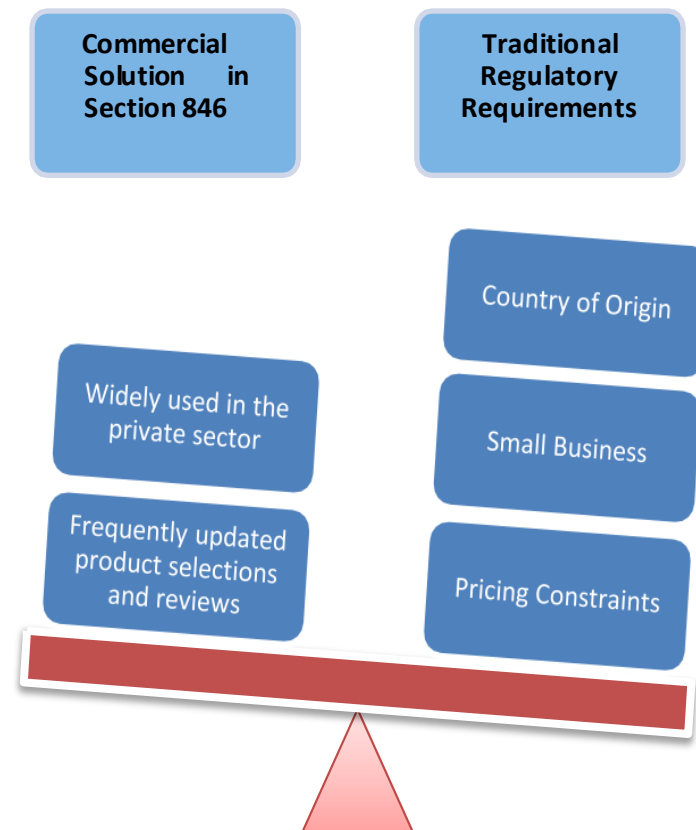
**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



E-Commerce Portal: NDAA 2018

The Weighing Game



E-Commerce Portal: NDAA 2018

Unsettled Questions

- How will the portals be selected?
- Will this be similar to the VA Prime Vendor Program?
 - Will portal holders have distribution contracts?
 - Fees?
 - flow-downs?
- How will program impact current federal contracts?
- Are there ecommerce marketplace options and distribution agreements?
- Some of the unknowns – risk and liability of e-commerce provider?

Federal Supply Schedules Transactional Data Reporting Rule:

- Established June 2016 – pilot program
 - Transactional level data on purchases made through GSA contract vehicle
 - Monthly reporting
 - Elements reported include, but not limited to:
 - price per unit of quantity sold
 - total price sold
 - Elimination of Price Reduction Clause (PRC) and Commercial Sales Practices (CSP)



**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



TDR

CSP/PRC

Reporting Sales

- Only report GSA sales to <https://tdr.gsa.gov>
- Report monthly at a transactional level
- Report what is on the invoice

- Only report GSA sales to <https://72a.gsa.gov>
- Report quarterly by summary

IFF Remittance

- Pay quarterly, have the option to pay monthly
- Same portal as where you report sales

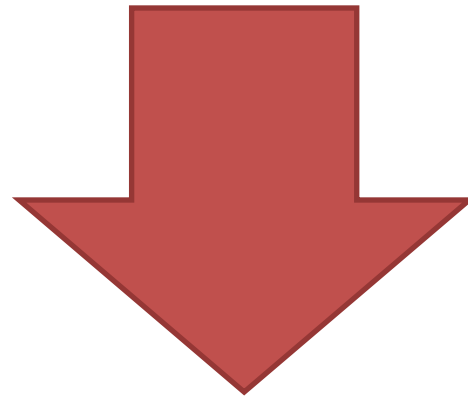
- Pay quarterly, NO option to pay monthly
- Same portal as where you report sales

Price Negotiation

- Pricing negotiated from comparison of like products and services (horizontal pricing)
- Removal of requirement to provide Commercial Sales Practices
- No pricing discount relationship created
- Removal of Price Reduction Clause and tracking requirement

- Provide all Commercial Sales Practices (vertical pricing)
- Establish a *Basis of Award Customer(s) and a Discount Ratio*
- If discount ratio is disturbed, trigger of the Price Reduction Clause

Federal Supply Schedules Transactional Data Reporting Rule:



- Additional reporting requirements
- Questions regarding use of data
- “Apples to apples” comparison



- Limited liability (CSP & PRC)
- No impact on commercial sales
- Removal of tracking customer



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Federal Supply Schedules

- New Rule on GSA Incidental Supply Schedule purchases
- Trade Agreements Act and the Department of Veterans Affairs
- VA Strategic Acquisition Center – Medical Surgical Prime Vendor-Next Generation

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Lorraine Campos

(202) 624-2786

lcampos@crowell.com

Chris Haile

(202) 624-2898

chaile@crowell.com

Rosamond Xiang

(202) 624-2613

rxiang@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Government Contracts IP: Developments and Trends

Jon Baker

John McCarthy

Chris Garcia

Charles Baek

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Legislative & Regulatory Updates

2018 NDAA – IP Provisions

- Section 802: IP within DoD
 - Requires DoD to develop IP acquisition and licensing policy that would enable coordination and consistency across DoD
 - Ensure program managers are aware of rules re IP rights allocations and that they fully consider and use all available techniques and best practices for acquiring/licensing IP early in the acquisition process
 - Encourage customized IP strategies for each system based on, at a minimum, the system's/component's unique characteristics, the product support strategy, the organic industrial base strategy, and the commercial market
 - Requires DoD to establish team of IP experts to be assigned to a program office

2018 NDAA – IP Provisions

- Section 835: Licensing of IP
 - Before selecting a contractor for engineering and manufacturing development or production of a major weapon system, DoD must negotiate a price for technical data to be delivered under the contract
 - Adds section to 10 U.S.C. § 2320 (re Rights in Technical Data) requiring DoD, “to the maximum extent practicable,” to negotiate and enter into specifically negotiated licenses for technical data to support the product support strategy of major weapon systems or subsystems

GSA Final Rule – Unenforceable Commercial Supplier Agreement Terms

- When: 83 FR 7631 issued on February 22, 2018
- What:
 - Declares certain Commercial Supplier Agreement terms unenforceable as inconsistent with federal procurement law. For example:
 1. Indemnification & Arbitration provisions
 2. Provisions subjecting USG to state law
 3. Automatic renewal provisions
 - Allows terms to be incorporated by reference (proposed rule required full text to be included with offer)
- Why: eliminates the need for negotiation on now unenforceable terms and facilitates faster procurements

NIST's Updates to Patent Rights Regulations

- The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) issued a series of changes to regulations implementing the Bayh-Dole Act (codified at 35 U.S.C. § 200 *et seq.*), which govern rights in inventions made under federal funding agreements
- 37 CFR 401, Rights to Inventions Made by Nonprofit Organizations and Small Business Firms under Government Grants, Contracts and Cooperative Agreements
 - Implements Bayh-Dole
 - NIST's updates applicable to 37 CFR 401

NIST's Updates to Patent Rights Regulations, Cont'd

- Effective May 14, 2018:
 1. No time limit on USG to demand title for untimely disclosed subject inventions (from 60 days → 0)
 2. Requires contractors to make inventor employees assign their patent rights
 3. More time for provisional applications: “automatic” one-year extension (unless agency denies within 60 days of request)
 4. Maintained requirement for substantial U.S. manufacture of subject inventions
 5. Confirmed Bayh-Dole’s application to large businesses
 6. Expands exceptions for the use of the standard patent rights clause

NIST's Updates to Patent Rights Regulations, Cont'd

- Bottom line:
 - Plenty of changes
 - Both substantive and timing related
 - Will changes be implemented in the FAR?

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Section 813 Government-Industry Advisory Panel Developments

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Government-Industry Advisory Panel

- Created pursuant to Sec. 813(b) of FY 2016 NDAA, as modified by Sec. 809(f) of FY 2017 NDAA
- Develop recommendations re laws and regulations relating to rights in technical data and computer software
 - Does not include patent rights

Government-Industry Advisory Panel

Appropriate consideration to the following factors:

- Ensure DoD does not pay more than once for the same work
- Ensure DoD contractors are rewarded for innovation & invention
- Provide for cost-effective reprocurement, sustainment, modification, and upgrades to DoD systems
- Ensure DoD has technical data rights necessary to support MOSA
 - Take into consideration the distinct characteristics of major system platforms, major system interfaces, and major system components developed exclusively with Federal funds, exclusively at private expense, and with a combination of Federal funds and private expense
- Encourage the private sector to invest in new products, technologies, and processes relevant to DoD missions
- Ensure that DoD has appropriate access to innovative products, technologies, and processes developed by the private sector for commercial use

Tension Point White Papers

- Organizes information to be addressed in Panel report
- Each tension point represents identified issue or conflict
 - Between existing law/regulation, and a desired state
 - Between Industry and Government
 - Between Industry and Industry
 - Prime contractors, subcontractors, component OEMs, repair contractors, and spares contractors
 - Between Government and Government
 - R&D laboratories, acquisition centers, sustainment centers
 - Need for data for Government use, publication purposes, depot use (sharing with depot contractors), competition (sharing with third parties)

Issues Considered – Tension Points

- Business model concerns – different business models in Government and industry create differing objectives
 - Include in solicitations the USG’s IP requirements, to the degree known
 - Share with Industry the USG’s priorities
 - When mixed funding exists, consider extending period of GPR or negotiate a SNL.
 - When USG requires more than the default licenses, it should negotiate a fair and reasonable price
- Acquisition planning and requirements – access for limited purposes (Cyber Review, Airworthiness Approvals) versus delivery as a CDRL

Issues Considered – Tension Points

- Source selection concerns
 - Data rights as an evaluation factor
 - Need for Government flexibility
- Balancing the interests of the parties
 - Indirect cost pools are considered privately funded
 - Treatment of IRAD
 - Funding test for rights
 - Commercial versus noncommercial
 - Commercial software terms versus Government-unique requirements
 - Authorized release and use of limited rights
 - Need for IP rights versus need for competition
 - Are existing rights for depots sufficient?

Issues Considered – Tension Points

- Implementation concerns
 - Differences between technical data and software
 - Development versus adaptation
 - FFF, technical data, software documentation
 - OMIT versus detailed manufacturing and process data (DMPD)
 - Rigid IP requirements versus need for flexible arrangements
 - Poor DID alignment with statutory/regulatory categories
 - 10 U.S.C. § 2321 protection versus complexity (link to source of funding alternatives)
 - Embedded software (object code) versus source code
 - Mandatory flow-down of clauses to commercial vendors/suppliers
 - **Right of first refusal regarding license rights for spare parts acquisition**



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Issues Considered – Tension Points

- Compliance/administrative concerns
 - Maintaining CDRL deliverables up to date
 - Small Business Innovation Research (SBIR)
 - Lack of trained personnel
 - Data assertion list
- Data acquisition concerns
 - Deferred ordering
 - Time limits on priced contract options
 - Deferred delivery versus escrow
- Modular Open Systems Architectures (MOSA) concerns
 - GPR in interfaces developed with mixed funding

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Tension Point Example

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

Section 813 Panel: Next Steps

- No set date for final report
- One open issue
- Report will likely be finalized in June
- Report will go to the OSD before going to Congress

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Contractors Going on the Offensive

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Oshkosh Defense, LLC v. U.S.

- Filed in U.S. Court of Federal Claims in March 2018, Case No. 18-404
- Alleges that USMC failed to follow DFARS 252.227-7037 procedures prior to removing restrictive markings
- Challenges USMC's unlimited rights determination



DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

Analytical Graphics, Inc. v. U.S.

- 135 Fed. Cl. 378 (2017) (Horn)
- Challenged, *inter alia*, USAF's decision to procure a non-commercial item for the Joint Inter-agency Combined Space Operations Center
- Agency required GPR, but Protester's commercial product was subject to commercial license

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Other Transaction Agreements

Prototype OT Authority

Per 2016 NDAA

- No DoD may use this prototype authority unless:
 - At least one nontraditional defense contractor participating to a significant extent;
 - All significant participants in the transaction are small businesses or nontraditional defense contractors;
 - At least one third of the total cost of the prototype project is to be paid out of funds provided by **parties to the transaction other than the Federal Government**; or
 - exceptional circumstances, not be feasible or appropriate under a contract, or would provide an opportunity to expand the defense supply base in a manner that would not be practical or feasible under a contract.

10 U.S.C. § 2371b(d)(1)

Prototype OT Authority

Per 2016 NDAA

- Nontraditional defense contractor = business unit that has not performed
 - CAS-covered contract for 1 year (10 U.S.C. § 2302(9))
 - ~~– any other contract in excess of \$500,000 to carry out federal prototype projects or to perform federal basic, applied, or advanced research projects~~

Prototype OT Authority

Per 2016 NDAA

- Prototype OT may provide for award of a follow-on production contract to the OT participants
 - May be awarded without competition if,
 - Competitive procedures used to select OTA participants, and
 - Participants successfully completed the prototype project
- Before 2016 NDAA, follow-on production had to be priced and scoped as part of the competitive OTA award process

Prototype OT Authority

2018 NDAA

- Section 216: More inclusive conditions for the use of OTA authority in several areas:
 - Significant participation by “at least one nontraditional defense contractor or nonprofit research institution” (emphasis added).
- Section 864 makes clear that prototype OTAs are for transactions.
 - Expands coverage of other transaction authority for a “prototype project” to “a transaction (for a prototype project)”
- Section 864 includes an expanded definition of “transaction”:
 - “A transaction includes all individual prototype subprojects awarded under the transaction to a consortium of the United States industry and academic institutions.” 10 U.S.C. § 2371b(f) (as amended)(emphasis added).

Prototype OT Authority

2018 NDAA, additional changes

- When cost share required, funding source expanded from parties to the transaction other than the Federal Government, to any non-Federal source.
- Increases the OTA approval thresholds
 - Increased maximum OTA approval authority of Senior Procurement Executive, Directors of DARPA or Missile Defense Agency from \$250M to \$500M.
 - Increased minimum threshold for obtaining OTA approval authority from Undersecretary of AT&L (with associated Congressional notification) from \$250M to \$500M.

Prototype OT Authority

Intellectual Property Guidance, 2017 DoD OT Prototype Guide

- Not required to comply within Bayh Dole (patents) or 10 USC § 2320-21 (technical data)
- However, other statutes may be applicable
 - FOIA, Trade Secrets Act
- In determining what rights to obtain, DoD should consider
 - Impact on life cycle costs, both in terms of royalty costs and the ability to obtain competition
 - Ability to use on other projects
 - Impact on attracting participants

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



QUESTIONS?

Charles Baek

(202) 624-2894

cbaek@crowell.com

Jon Baker

(202) 624-2641

jbaker@crowell.com

Chris Garcia

(213) 443-5526

cgarcia@crowell.com

John McCarthy

(202) 624-2579

jmccarthy@crowell.com

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)



Global Operations in a Time of Bold Trade Rhetoric

Addie Cliffe

Jana del-Cerro

Cari Stinebower

The Trump Administration and Trade Policy

- Is “America First” a cohesive trade policy?
- What does it mean for government procurement?



China in the Crosshairs

- Committee on Foreign Investment in the U.S. (CFIUS)
- Section 301 Report
- Extension of ban on Huawei, ZTE
- Qualified Products List and DLA policy
- Supply chain security
 - *Iron Bow v. United States*

Domestic Preferences: Strengthening or Relaxing?

- Pending Buy American legislation to tighten up
- Renegotiation of trade agreements
- GSA/OMB joint proposal re e-commerce and increasing the micro-purchase threshold

Export Controls

- **Export Control Reform marches on?**
 - Rounding out the USML revisions (Categories I-III), refreshing/revising USML going forward
 - Export control modernization - DDTC moving to automated forms VSDs/M&A notices, web-based CJs
 - BIS intrusion and surveillance rule/ Wassenaar updates
- **Other priorities in new Administration?**
 - Export Control Reform Act?
 - New CCL controls on emerging technology

Sanctions

- **Iran whiplash**
 - Withdrawal from the JCPOA
- **Unpredictability with Russia**
 - Temporary chaos in aluminum markets
 - Secondary sanctions for non-US parties
 - More designations to come?
- **North Korea**
 - Method and pace of denuclearization ?
- **Venezuela**
 - Expanded list-based sanctions

DIVING INTO
UNCHARTED WATERS

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Addie Cliffe

(202) 624-2816

acliffe@crowell.com

Jana del-Cerro

(202) 624-2843

mdel-cerro@crowell.com

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Accounting, Cost & Pricing

Nicole Owren-Wiest

Liz Buehler

Outline

- DCAA and 2018 NDAA
- Recent Final Rules
- 2016 NDAA Section 809 Panel Update
- Litigation Costs from Discrimination Lawsuits
- Contractor Recovery of Interest

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



DCAA and 2018 NDAA

2018 NDAA – Incurred Cost Audits

- Section 803
 - Requires DoD to comply with commercially accepted standards of risk and materiality in performance of audits and
 - Requires DoD to implement numeric materiality standards for audits by 10/1/2020 after consultation with auditors and Section 809 panel

2018 NDAA – Incurred Cost Audits

- Section 803
 - Requires DoD to use “qualified private auditors” to perform a “sufficient number” of audits so DCAA can focus on higher-risk and more complex audits
 - Implementation plan due October 1, 2018
 - Contracts to be awarded by April 1, 2019

2018 NDAA – Incurred Cost Audits

- Section 803
 - Prescribes timelines for timely audit of incurred cost submissions
 - 60 days after ICS: notify contractor whether qualified
 - Within 1 year from submission of qualified ICS: Complete audit and issue findings
 - By 10/1/2020, if audit findings not issued in 1 year, then audit “shall be” considered complete and no additional audit work may be performed (subject to reporting requirements, Director of DCAA may waive requirement on a case-by-case basis)

2018 NDAA – Cost or Pricing Data Requirements

- Section 811
 - Raises threshold from \$750,000 to \$2 million (TINA and CAS)
 - Modifies authority to require submission of other than cost or pricing data
- DoD Class Deviation 2018-00012
 - Issued April 13, 2018
 - Effective July 1, 2018, COs must “use \$2 million as the threshold for obtaining” certified cost or pricing data; also implements for CAS

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Recently Issued Final Rules

Audit of Termination Settlement Proposals

- On May 1, 2018, the FAR Council issued a final rule amending FAR 49.107
- Increases threshold for mandatory audit of prime contract TSPs, as well as subcontractor TSPs, from \$100,000 to the TINA threshold (currently \$750,000, but \$2M as of July 1)
- Effective May 31, 2018

Promoting Voluntary Disclosure of Defective Pricing

- On May 4, 2018, DoD issued a final rule, effective immediately, amending the DFARS to give DoD COs more leeway in evaluating contractors' post-award defective pricing disclosures
- Requires only a discussion between the CO and DCAA to determine whether a limited-scope audit, full-scope audit, or technical assistance is appropriate for the circumstances

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



2016 NDAA Section 809 Panel Update

2016 NDAA Section 809 Panel Update

- Team 9 (Cost Accounting Standards) Recommendations
 - CAS Applicability, Exemptions, Thresholds
 - Definitions of CASB Terms
 - Relocation and Composition of CAS Board
 - Offsetting multiple changes

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Litigation Costs

Litigation Costs from Discrimination Lawsuits

- *Bechtel Nat'l, Inc. v. United States*, No. 17-657C
 - Concerned litigation costs that Bechtel incurred to defend two discrimination lawsuits
 - Under *Tecom*, legal fees and costs incurred in connection with settling a private action for employment discrimination unrelated to fraud will be allowable only if the contractor can establish that the private plaintiff had very little likelihood of success on the merits
 - Bechtel argued that *Tecom* was not applicable because the contract at issue contained a clause stating that a contractor “shall be reimbursed...[f]or liabilities...to third persons.”
 - The COFC disagreed, finding that the same clause contained an exception making the allowability of those costs “dependent upon whether they are otherwise allowable under the terms of the contract, a determination to which *Tecom* speaks with respect to contracts that include non-discrimination clauses....”

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)



Recovery of Interest on Contractor Claims for Disallowed and Withheld Indirect Costs

Contractor Recovery of Interest

- Normally in cost allowability litigation, the government is seeking to recover costs that have already been paid to the contractor, so there is no issue about whether CDA interest is due to the contractor
- In some cases, the government may withhold costs on current and future contracts, or recoup prior period costs, pending the result of litigation
- To recover interest, contractor must file a certified claim for the amount withheld and/or recouped by the government
- Contractor is entitled to CDA interest from the date of the claim to the date of payment (including interest on amounts not yet incurred at the time of the claim)

Contractor Recovery of Interest

- Notable Cases
 - *Bath Iron Works*, ASBCA No. 32770 (1987)
 - *Servidone Constr. Corp. v. United States*, 931 F.2d 860 (Fed. Cir. 1991)
 - *Caldera v. J.S. Alberici Contr. Co.*, 153 F.3d 1381 (Fed. Cir. 1998)
 - *Daewoo Eng'g and Const. Co., Ltd. v. United States*, 557 F.3d 1332 (Fed. Cir. 2009)

**DIVING INTO
UNCHARTED WATERS**

Ounce of Prevention Seminar (OOPS)

QUESTIONS?

Liz Buehler

(202) 624-2821

ebuehler@crowell.com

Nicole Owren-Wiest

(202) 624-2863

nowrenwiest@crowell.com

Cari Stinebower

(202) 624-2757

cstinebower@crowell.com