



High Risk Compliance Pitfalls in Federal Government Contracts: How to Spot, Avoid, and Mitigate

September 23, 2021



Speakers



Adam Lasky

Partner & Co-Chair
Government Contracts
Seyfarth Shaw LLP



Kelli Hooke

Senior Corporate Counsel, Legal Compliance
Public Sector Compliance
T-Mobile

Agenda



- Vexing and High-Risk Compliance Problems
 - Service Contract Act
 - Supply chain
 - Cybersecurity
 - Mergers & Acquisitions
- Actions Once Non-Compliance is Reported or Suspected
 - Mandatory disclosures
 - Internal investigations
 - Responding to SDOs



Service Contract Act

What's Service Contract Act



- Service Contract Labor Standards Act
 - aka McNamara-O'Hara Service Contract Act or SCA
- Prevailing wage law applicable to federal service contracts
 - Contract predominantly performed by service employees
 - Wages
 - Benefits

Why is SCA High Risk?



- Amongst the most complex statutory/regulatory scheme in GovCon
- Unlike construction contractors, service contractors aren't used to prevailing wage laws in state/local government contracting
- Fluctuating levels of enforcement based on White House political party and some rules are counter-intuitive
- Small violations can have enormous penalties
- Risk of major contract financial losses if bidding without understand SCA
- Much higher suspension & debarment risk
 - “Present responsibility” not a viable defense
- False Claims Act risk

Common SCA Pitfalls

What to Watch Out For



- Not recognizing that the contract is covered by SCA
 - Or not objecting pre-bid to inclusion of SCA clause to a services contract that shouldn't be covered by SCA
- Using incorrect WD or incorrect WD job classifications
- Counting fringe payments that aren't "bona fide" fringe (many health and pension plans don't meet SCA requirements, or must receive specific DOL approval)
- Failing to cash out remaining vacation at end of year
- Overpayment of H&W benefits (for work above 40/2080 hours)
- Failing to flow-down SCA requirements to subcontractors (joint/several liability)
- Not adequately/tracking segregation of employee time between SCA and Non-SCA covered work
- Failure to understand or account for successor-in-interest CBA rules
- Failure to price multi-year option contract labor in accordance with SCA principles
- WD inaccurate and workforce not unionized



Supply Chain

**Best Practices and NIST Standards
A Multi-Disciplinary Endeavor**

Supply Chain Threat Groups



- **Counterfeit Parts/Tampering.** Insertion of counterfeits or tampering with supplier components, products, or services in the supply chain.
- **Cybersecurity.** External attacks on suppliers' operations and capabilities, exploit vulnerabilities, or plant malware.
- **Internal Security Ops & Controls.** Weaknesses in internal supplier processes lead to weaknesses in basic cyber hygiene, user awareness, mishandling of information.
- **End-to-End.** Environmental, geographical, regulatory compliance, workforce, and other vulnerabilities to the confidentiality, integrity, or availability of supplier information, products, or services.
- **Insider Threat.** Vulnerability of the supplier to attack from trusted staff and partners within the organization.
- **Economic.** Issues with financial viability of suppliers and potential impact to supply chain integrity resulting from failure of key supplier.

Risk: A Lot to Manage



- Type of Labor
 - Combating trafficking in persons
 - Certification regarding knowledge of child labor for listed end products
- Type of Equipment
 - Prohibition on contracting for hardware, software, and services developed or provided by Kaspersky Lab
 - Sec. 889 prohibition on covered Telecom
- Type of Vendor
 - Prohibition on using suspended or debarred companies

Bonus: The always complicated BAA and TAA requirements

National Institute of Standards & Technology



- Special Publication 800-161
- SCRM Practices for Federal Information Systems and Organizations
 - ICT guidance on supply chain risk management
 - 19 Control Families
 - 250 Security Controls

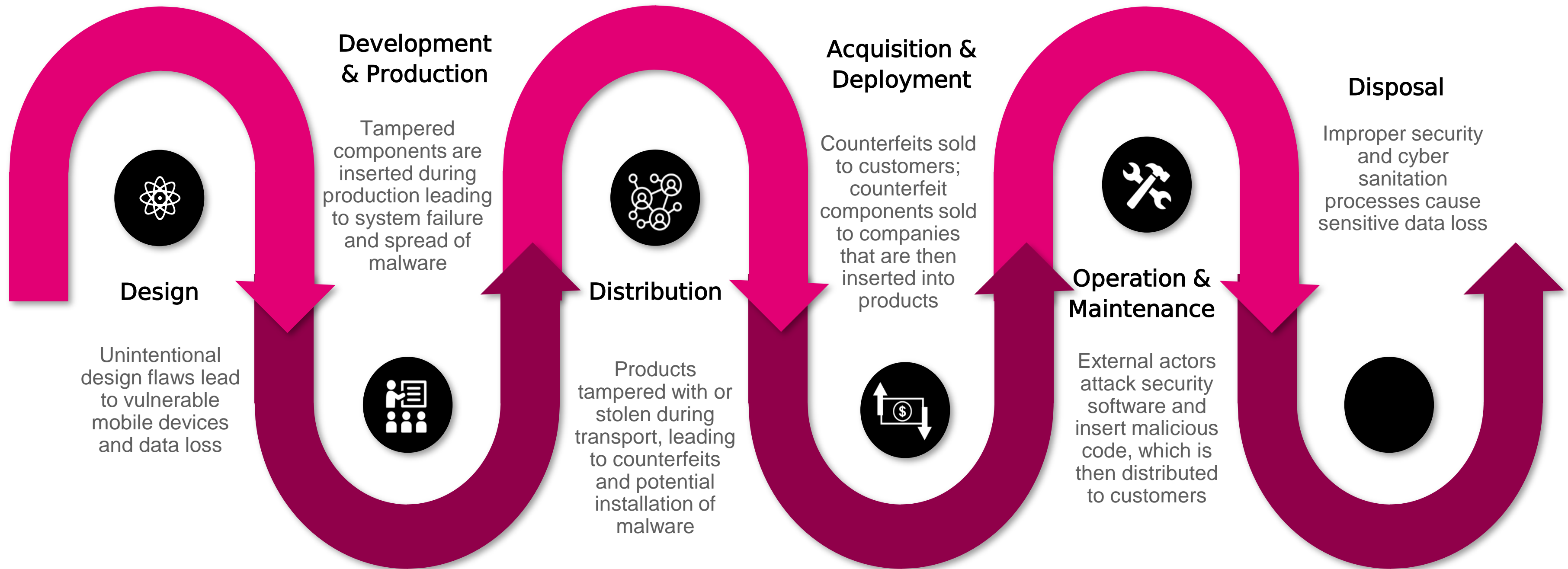
NIST SP 800-161 Security Control Families	
Access Control (AC)	Physical and Environmental Protection (PE)
Awareness and Training (AT)	Planning (PL)
Audit and Accountability (AU)	Program Management (PM)
Security Assessment and Authorization (CA)	Personnel Security (PS)
Configuration Management (CM)	Provenance (PV)
Contingency Planning (CP)	Risk Assessment (RA)
Identification and Authentication (IA)	System and Services Acquisition (SA)
Incident Response (IR)	System and Communications Protection (SC)
Maintenance (MA)	System Information Integrity (SI)
Media Protection (MP)	



Cybersecurity

Threat Events Across the ICT Life Cycle

Threat Source + Vulnerability = **Threat Event**



Industry & Government Standards



- NIST Standards
 - 800-53
 - 800-171
- FAR and DFARS
- Cyber Maturity Model Certification
- Good old fashion cyber hygiene

Cyber Maturity Model Certification

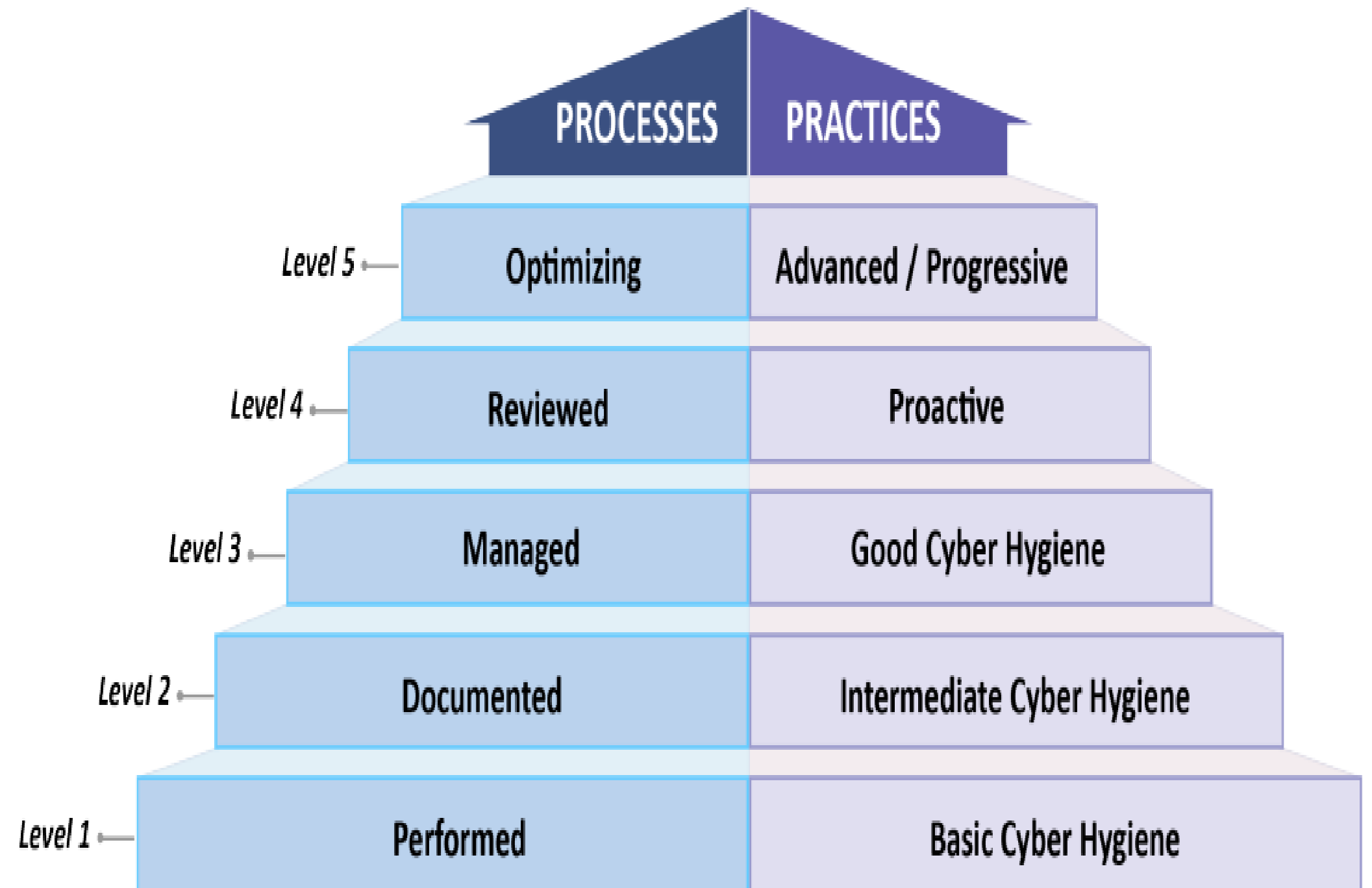


Figure 2. CMMC Levels and Descriptions



Mergers & Acquisitions

Buying or Selling a Government Contractor

Why is GovCon M&A High Risk?



- Many GovCon M&A transactions require pre-approval or notice to the Government
- Government officials charged with approval are slow and sometimes don't understand approval rules
- Some M&A attorneys don't know the specific GovCon M&A rules (and very few know the SBA GovCon specific M&A rules)
- Non-compliance can result in:
 - termination of contracts
 - ineligibility for future contracts
 - disqualification from procurements with pending proposals
 - bid protest risk
 - False Claims Act liability
 - Suspension or Debarment (including affiliates)
- Purchasing a government contractor may turn your entire family of companies into a “government contractor” for certain regulatory compliance purposes
- Rule of thumb for buyers – don't assume the seller knows what is required

Novations



- Anti-Assignment Act
- Asset Sale (buyer purchases all or some of seller's assets)
 - Novation required
- Stock Sale (seller is stockholder, and buyer purchases seller's stock and sold company continues to exist under new ownership)
 - Novation not required (though some Gov't customers will dispute this)
 - Notice (potential pre-approval if seller is status-based small business)
- Merger (two entities combine into buying entity, the selling-entity dissolves --- seller's contracts must be transferred "by operation of law")
 - Novation *may* be required
 - Case law says Anti-Assignment Act doesn't apply to mergers
 - But the FAR says otherwise
 - specifically lists "transfer of ... assets incident to a merger or corporate consolidation" as a transaction requiring a novation agreement

Buying or Selling a Gov't Contractor Involved In SBA Programs



- Double the Red Tape
- Affiliation/Certification rules
- Present Effect Rule
- Special Rules for Unrestricted MACs & Joint Ventures
- Status-Held Small Businesses – Extra Restrictions
 - Governing Agency Approval of Transaction
 - 8(a) Program Participants (or former Participants' still holding an 8(a) contract)
 - SBA Pre-Approval [13 CFR 124.515]
 - Contract transfers require SBA waiver – very limited authority to grant
 - SDVOSB (CVE) – VA Post-Approval, 30 days [38 CFR 74.3]
 - Direct Ownership (SDVOSB, WOSB, 8(a))

Impact on Pending Proposals



- Procurement agency must consider “imminent and essentially certain” transactions in procurement evaluation that occur before award
- Material Misrepresentation doctrine
- May create a notice obligation
- May create a basis/obligation for agency to eliminate proposal
- Bid protest risk
- Loss of standing to protest



Mandatory Disclosures

FAR 52.2003-13



2) *The Contractor shall –*

- ii. Exercise due diligence to prevent and detect criminal conduct; and
- iii. Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law

3)

- ii. The Contractor shall timely disclose, in writing, to the agency, Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed –
 - A. A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States code; or
 - B. A violation of the civil False Claims Act (31 U.S.C. 3729-3733)

Why Disclose?



- The relevant regulation or law states you must report
- Prevent an allegation of a False Claim Act violation by an intervenor or other party
- Voluntary Disclosures?
- To whom: the appropriate government authorities
 - Law enforcement
 - Program officials
 - Regulators



Internal Investigations

Why Investigate?



- To address alleged misconduct
 - Hotline call
 - Employee talks to management
 - Receive information a vendor has not complied
- Demonstrate an effective compliance and ethics program
- Prevent False Claims Act actions

How to Investigate?



- Key considerations:
 - Inside or outside counsel
 - Maintain privileged
 - Upjohn for everyone
- Follow with remediation
- Refer to Mandatory Disclosures discussion



Suspension & Debarment Responding to SDOs

What is S&D



- The government contracts “corporate death penalty”
- Suspension
 - a temporary (indefinite) disqualification of a contractor from government contracting
- Proposed debarment
 - occurs when an agency debarring official issues a notice of proposed debarment, and lasts until the debarring official makes the decision on whether or not to debar for a specified period
- Debarment
 - an exclusion of a contractor from government contracting for a specified period after debarment procedures have been followed (generally not exceed 6 years)
- S&D actions can be taken against offending company’s affiliates
- Federal-wide debarment
 - And covers most subcontracting
- Cross-debarment
- Usually starts w/ letter from SDO

Pre-emptive steps to reduce S&D risk from future misconduct



- Implement formal “values-based” ethics program
 - review and control procedures
 - training
 - encourages employees to “do the right thing.”
 - Company-wide commitment to the ethics program
 - senior management commitment and involvement with program
- Designated company ethics officer

How to avoid S&D after misconduct has occurred



- Choose your adventure – Contest vs Acknowledge/Mitigate
- Understand before you choose:
 - Understand the “present responsibility” test (except SCA)
 - Understand limits on judicial review
 - Understand the difficulty in obtaining judicial relief
 - Business disruption and collateral liability risks of Acknowledge/Mitigate approach

How to avoid S&D after misconduct has occurred



- Acknowledge/Mitigate Approach – Key factors that SDO will consider in present responsibility analysis
 - Effective standards in control in place (or adopted)
 - Self-disclosure and degree of cooperation
 - Prompt payment of all fines/sanctions or other monetary obligations
 - Appropriate disciplinary action against individuals involved
 - Implementation of effective remedial measures (and time since offence)
 - Acknowledgment of responsibility and recognition of seriousness of the misconduct
 - Administrative agreements
- *Don't wait until you receive a letter from the SDO*



Questions?

Speaker Contact



Adam Lasky

Partner & Co-Chair
Government Contracts
Seyfarth Shaw LLP
(206) 946-4945
alasky@seyfarth.com



Kelli Hooke

Senior Corporate Counsel, Legal Compliance
Public Sector Compliance
T-Mobile
(425) 624-3036
Kelli.Hooke2@t-mobile.com