Strategic Legal Partners, LLC

Virtual General Counsel for Modern Businesses & Federal Contractors

GOVCON LEGAL BULLETIN — APRIL 2026

Critical Legal Developments Every Small Business Federal Contractor Must Know — April 2026

From the Desk of Strategic Legal Partners:

The federal contracting landscape has shifted materially in recent months. Five overlapping legal developments — a sweeping new DEI Executive Order, expanding cybersecurity enforcement, mass contract terminations, new agency fraud enforcement authority, and a major defense spending bill — are creating real, immediate risk for small business government contractors. This bulletin explains what is happening, what it means for your business, and what you should do right now. Our goal is what it has always been: keeping you proactive, protected, and positioned to grow.

1. DEI Executive Order — New Contractor Obligations URGENT

What happened: On March 26, 2026, President Trump signed an Executive Order titled *Addressing DEI Discrimination by Federal Contractors*. The Order mandates elimination of DEI programs for all federal contractors and subcontractors, and it carries serious consequences for noncompliance.

Why it matters to you:

- Your contract may be terminated, suspended, or cancelled for noncompliance.
- You are now legally required to report known DEI conduct by your subcontractors to the contracting agency.
- Compliance is tied directly to the False Claims Act — billing the government while out of compliance could expose you to treble damages and civil penalties under 31 U.S.C. § 3729.
- The FAR Council has 60 days to issue implementing regulations and new contract clauses — this clock is already running.

Large Business Contractors

- Must audit all internal DEI programs enterprise-wide
- Responsible for subcontractor DEI reporting obligations
- Expect new contract clause language in all solicitations within 60 days

Small Business Contractors

- DEI programs are common in teaming and SBA set-aside contexts — review now
- Do not terminate employees or programs without counsel — employment law risk applies
- Update subcontract templates before new FAR clauses issue

Your Action Items — Act Before the 60-Day Regulatory Deadline

- Conduct an immediate audit of all DEI-related policies, hiring programs, and training materials
- Review all teaming agreements and subcontracts for DEI exposure
- Do not take unilateral remedial action without consulting counsel first
- Monitor FAR Council guidance expected within 60 days and update contract templates accordingly

2. CMMC Cybersecurity Certification — FCA Liability Is Now Real

URGENT

What happened: The DoD's Cybersecurity Maturity Model Certification (CMMC) framework went live November 10, 2025. If you hold a DoD contract, a senior executive at your company must now annually certify your cybersecurity compliance in the SPRS database. An inaccurate affirmation — even due to reckless oversight — can constitute a False Claims Act violation.

The enforcement numbers are serious:

- DOJ recovered $52 million across 9 cybersecurity FCA settlements in FY2025.
- In December 2025, a small subcontractor paid $421,000 for inadequate cybersecurity of technical drawings — enforcement has reached the supply chain.
- DOJ has confirmed: these cases are about misrepresentations, not data breaches. Your exposure exists even if you have never had a breach.
- Phase 2 arrives November 10, 2026 — Level 2 contractors must have third-party (C3PAO) assessments. Assessor slots are filling now.

Prime Contractors

- Annual executive affirmation must reflect verified compliance — not assumed
- M&A due diligence must now include CMMC compliance history of acquisition targets
- Begin C3PAO engagement immediately — Phase 2 is 7 months away

Subcontractors

- Enforcement reaches you directly — the $421K December 2025 settlement was a subcontractor
- Identify your CMMC level based on whether your systems handle FCI or CUI
- Do not self-attest compliance without first conducting a gap assessment

Your Action Items — Phase 2 Deadline: November 10, 2026

- Determine your CMMC level (Level 1, 2, or 3) based on your contract information type
- Verify your actual cybersecurity posture against NIST SP 800-171 before any executive signs the SPRS affirmation
- If you handle CUI at Level 2, engage a C3PAO assessor now — demand is rising and slots are limited
- Contact us before responding to any government inquiry about cybersecurity compliance

3. DOGE Contract Terminations — Know Your Rights and Recovery Options

What happened: Over 6,000 federal contracts have been terminated since January 2025, and small businesses — particularly women-owned, minority-owned, HUBZone, and SDVOSB firms — are bearing a disproportionate share of the impact. Terminations are issued as "terminations for convenience" under FAR 52.249-1.

A termination for convenience does not eliminate your right to compensation. Under FAR Part 49, you are entitled to recover reasonable costs, settlement expenses, and profit on work completed. You must file a termination settlement proposal — typically within 120 days. Missing this deadline can forfeit your recovery rights entirely.

What you should know:

- 35–40% of cancelled contracts are historically re-competed within 12–18 months, often with set-aside designations.
- Agencies remain bound by statutory small business goals: 23% of prime contract dollars, 5% for 8(a), 3% for HUBZone, 3% for SDVOSB, and 5% for WOSB.
- USAID (68%), Dept. of Education (52%), and EPA (41%) have seen the largest proportional cuts — if you serve those agencies, assess your pipeline now.

Your Action Items — The 120-Day Clock Starts at Termination

- If you receive a termination notice, contact us immediately to preserve your recovery rights
- Document all costs incurred and work performed as of the termination effective date
- Monitor SAM.gov for re-solicitations in your NAICS codes from cancelled contracts
- Review your pipeline diversification — this is the time to assess agency concentration risk

4. Administrative False Claims Act — Agencies Now Pursue Smaller Cases Directly

What happened: The Civilian Board of Contract Appeals has issued new procedural rules implementing the Administrative False Claims Act, giving federal agencies direct authority to pursue smaller-value fraud cases — without DOJ involvement. Previously, low-dollar matters rarely resulted in formal proceedings. That is no longer the case.

For small businesses performing cost-reimbursement or time-and-materials contracts, this means billing irregularities, cost mischarging, or minor compliance gaps are now more likely to trigger formal agency proceedings. Self-correction before submission has never been more important.

Your Action Items

- Review invoicing practices on all cost-type and time-and-materials contracts for accuracy and completeness

- Implement internal review controls to catch billing errors before submission
- Establish a documented process for identifying and voluntarily correcting errors — this is significantly less costly than responding to agency enforcement

5. FY2026 NDAA & FAR Overhaul — Opportunities and Supply Chain Risk

What happened: The FY2026 National Defense Authorization Act (NDAA), signed December 18, 2025, authorizes $900+ billion in defense funding and raises key acquisition thresholds — reducing certain administrative and pricing disclosure burdens for contractors. At the same time, the BIOSECURE Act provisions embedded in the NDAA create new supply chain compliance obligations that many small businesses are unaware of.

The opportunity:

- Higher thresholds for the Truthful Cost or Pricing Data Act (TINA) and Cost Accounting Standards reduce certified cost-or-pricing data requirements on mid-range contracts.
- Increased noncompetitive acquisition thresholds may create more sole-source opportunities for qualifying small businesses.
- The ongoing FAR overhaul is removing non-statutory compliance provisions — reducing paperwork burdens across the board.

The risk:

- The BIOSECURE Act creates supply chain scrutiny that reaches software tools, IT platforms, data systems, and subcontractors with ties to restricted foreign entities.
- Many small businesses are unaware of their exposure at the software and services layer — this risk can disqualify an otherwise compliant contractor.

Your Action Items

- Review the new TINA and CAS thresholds with your pricing team — you may no longer need certified cost data on certain proposals
- Audit your third-party vendors, software, and subcontractors for BIOSECURE Act exposure
- Track FAR overhaul rulemaking to identify which compliance obligations are being retired versus which remain mandatory under statute

Why This Matters for Our Clients

Most small businesses engage legal counsel reactively — after a problem has already materialized. These five developments illustrate exactly why that model fails in federal contracting. By the time a CMMC affirmation triggers an FCA investigation, a DEI policy creates contract suspension risk, or a termination deadline passes, the cost of inaction has multiplied.

Strategic Legal Partners was built for exactly this environment. As your embedded Virtual General Counsel, we identify these developments as they happen, assess their impact on your specific contracts, and help you act before risk becomes liability. Our subscription model means you have continuous legal guidance — not episodic counsel after the fact.

Integrated Legal Strategy. Real Partnership. Predictable Cost.

Schedule Your Strategy Call

These developments require proactive action — not a wait-and-see approach. As your Virtual General Counsel, Strategic Legal Partners is ready to assess your specific exposure and guide your next steps.

www.strategiclegalpartners.com