Government Contracts Year In Review (2025)

Speakers:

- Nick Solosky, Partner, Fox Rothschild
- Michael Bauer, General Counsel, Versar, Inc
- Michael Vozzo, Senior Director of Litigation Management and Strategy, Constellis

© 2025 Fox Rothschild LLP

Agenda

- Bid Protest Standing & Jurisdiction
- Project Labor Agreements
- Proposal Evaluation & SAM Registration Pitfalls
- Enforcement & Cyber Compliance
- Practical Takeaways for 2026

Standing and Jurisdiction

Bid Protest Standing

Other Transaction Authority

© 2025 Fox Rothschild LLP

Percipient.ai, Inc. v. United States (Fed. Cir. En banc) August 28, 2025

III

"In construing a statute or regulation, we begin by reviewing its language to ascertain its plain meaning." *Am. Airlines, Inc. v. United States*, 551 F.3d 1294, 1299 (Fed. Cir. 2008). Section 1491(b)(1) reads:

> Both the Unite[d] States Court of Federal Claims and the district courts of the United States shall have jurisdiction to render judgment on an action by *an interested party* objecting to a solicitation by a Federal agency for bids or proposals for a proposed contract or to a proposed award or the award of a contract or any alleged violation of statute or regulation in connection with a procurement or a proposed procurement. Both the United States Court of Federal Claims and the district courts of the United States shall have jurisdiction to entertain such an action without regard to whether suit is instituted before or after the contract is awarded.

Percipient.ai, Inc. v. United States (Fed. Cir. En banc) August 28, 2025

Key Legal Issue

Who qualifies as an "interested party" eligible to bring a bid protest under 28 U.S.C. § 1491(b)(1)?

Understanding the Context:

- The National Geospatial-Intelligence Agency (NGA) issued a solicitation (SAFFIRE) for advanced geospatial intelligence technology.
- CACI, Inc.-Federal was awarded the contract. Percipient.ai (a computer vision (CV) technology provider) did not bid because it could not meet all solicitation requirements.
- Percipient.ai later sought to challenge NGA's compliance with statutory requirements favoring commercial products, arguing its CV platform should have been considered.

Percipient.ai, Inc. v. United States: Flashback

- Percipient.ai, Inc. v. United States, 104 F.4th 839, 851 (Fed. Cir. 2024)
- The Court ruled for protester based on the expansive language of the Tucker Act permitting protests of "any alleged violation of statute or regulation in connection with a procurement or proposed procurement." Previously, only interested parties could file a protest and even interested parties could not file a protest on a task order award (the Task Order Protest Bar). Percipient.ai, Inc. v. United States, 104 F.4th 839, 851 (Fed. Cir. 2024).
- "[T]he Percipient decision, like **Loper Bright**, emphasized the courts' primacy in interpreting the law, and so Percipient may turn out to have been one of the first decisions which follows Loper Bright's trajectory and opens new lines of challenges to agency procurement decisions, grounded in the courts' Prerogative to define what the law is."

Percipient.ai, Inc. v. United States: Holding

- The en banc court held that only "actual or prospective bidders or offerors whose direct economic interest would be affected by the award of the contract or by failure to award the contract" qualify as "interested parties." Affirms dismissal of underlying protest for lack of standing.
- The court rejected arguments to expand standing to subcontractors or other parties not directly bidding.
- The court relied on the statutory language of § 1491(b)(1), the Competition in Contracting Act (CICA), and longstanding precedent.
- The decision emphasized that Congress had considered and rejected broader definitions of "interested party" in prior legislative history.

Percipient.ai, Inc. v. United States: Significance

- The decision definitively limits standing in the Court of Federal Claims to actual or prospective bidders or offerors, excluding subcontractors and other indirectly interested parties.
- This provides clear guidance for who may challenge federal procurement actions, reducing uncertainty and potential litigation from peripheral parties.
- The court's approach ensures consistent interpretation of "interested party" across procurement statutes, aligning with CICA and prior case law.
- The ruling rejects attempts to broaden standing through creative statutory interpretation, emphasizing the importance of legislative intent.

Percipient.ai, Inc. v. United States: Dissent

- The dissent contends that the majority's "one-size-fits-all" approach—limiting "interested party" to actual or prospective bidders for all types of challenges—ignores Congress's broader language.
- Points out that even the government conceded at oral argument that the group of "interested parties" could differ depending on the type of challenge.

Telesto Group, LLC v. United States, No. 1:24-cv-01784 (COFC Jun. 2, 2025)

GOVERNMENT CONTRACTING LAW REPORT

Seeking Connection (to a Procurement or Proposed Procurement): The Jurisdictional Hook for OTA Protests

By Nicholas T. Solosky and Keeley A. McCarty*

As federal agencies increasingly rely on Other Transaction Authority (OTA) to speed innovation and bypass traditional procurement hurdles, legal challenges to OTA awards are also on the rise. But where can contractors turn when they believe an OTA award is unfair or unlawful? In this article, the authors provide a timely, in-depth analysis of OTA bid protest jurisdiction across the U.S. Court of Federal Claims (COFC), the Government Accountability Office, and federal district courts. Geared toward federal contractors, the authors offer strategic insights into protest viability, jurisdictional traps, and the legal gray zone between nontraditional acquisitions and traditional procurement oversight.

Telesto Group, LLC v. United States

Key Legal Issue

Under what circumstances does the COFC have bid protest jurisdiction under 28 U.S.C. § 1491(b)(1) for Other Transaction Agreements (OTA).

This case is significant for government contractors as it delineates the boundaries of judicial review for OTAs and provides practical guidance for both agencies and contractors navigating the increasingly common OTA procurement landscape.

Telesto Group, LLC v. United States: OTA Primer

Understanding the Context:

- OTAs offer the chance to bypass traditional procurement rules. A flexible contracting mechanism that can also be used to accelerate innovation and collaboration with non-traditional government vendors.
- Key drivers behind the proliferation of OTA authority include:
    - *Flexibility and Speed*
    - *Attracting Non-Traditional Contractor Prototyping and Innovation*

Telesto Group, LLC v. United States: Holding

Limited Jurisdiction Over OT Protests:

- The COFC held that its jurisdiction over protests involving "other transaction" (OT) authority projects under 10 U.S.C. § 4022 is limited – but COFC is still the “de facto” destination.

Procurement vs. Non-Procurement:

- The court distinguished between OTAs that are not procurements and those that become procurements when the agency decides to acquire a successful prototype through a follow-on production contract.

Jurisdictional Blackout During Prototyping:

- The COFC lacks jurisdiction to review the agency’s conduct or evaluations during the prototyping phase of an OT project. Jurisdiction arises only after the prototyping phase is completed and the agency decides to proceed with a follow-on production contract.

Project Labor Agreements

© 2025 Fox Rothschild LLP

MVL USA, Inc. et al. v. United States, No. 24-1057 (Fed. Cl. Jan. 21, 2025)

Key Legal Issue

Do mandatory project labor agreements (PLA) on large-scale federal contracts violate the Competition in Contracting Act (CICA).

Arises out of Biden-era Executive Order 14063 in February 2022, instructing federal agencies to require construction contractors and subcontractors on projects valued at $35 million or more to “agree, for that project, to negotiate or become a party to” a PLA.

MVL USA, Inc. et al. v. United States

- The court found that the use of a PLA in this procurement violated CICA.
- CICA requires that federal agencies obtain “full and open competition” in their procurements unless a specific statutory exception applies.
- The court determined that mandating a PLA effectively limited the pool of potential bidders, as non-union contractors or those unwilling to agree to the PLA terms were excluded or deterred from bidding.

Small Business Compliance

© 2025 Fox Rothschild LLP

Size Appeal Of: Decisionpoint-Agile Defense JV, LLC

Key Legal Issue

Whether the SBA area office erred by failing to consider the terms of a joint venture operating agreement (OA) for purposes of a size determination – even where the OA was not explicitly incorporated into the main joint venture agreement.

Size Appeal Of: Decisionpoint-Agile Defense JV, LLC

Context:

- Protest questioned whether the JVA / OA together satisfy the regulatory requirements for mentor-protégé JVs under 13 C.F.R. § 125.8(b)(2), including:
  - Designation of managing venturer & responsible manager with ultimate responsibility for contract performance
  - Specification of major equipment, facilities, other resources to be contributed by each venturer.
  - Obligation to complete performance even if a venturer withdraws.

OHA held that the Area Office erred by ignoring the OA simply because it was not incorporated into the JVA. The OA is a fundamental governing document of the entity and must be considered if executed before the date of final proposal submission.

(b) ***Contents of joint venture agreement.***

(1) A joint venture agreement between two or more entities that individually qualify as small need not be in any specific form or contain any specific conditions in order for the joint venture to qualify as a small business.

(2) Every joint venture agreement to perform a contract set aside or reserved for small business between a protégé small business and its SBA-approved mentor authorized by § 125.9 must contain a provision:

(i) Setting forth the purpose of the joint venture;

(ii) Designating a small business as the managing venturer of the joint venture, and designating a named employee of the small business managing venturer as the manager with ultimate responsibility for performance of the contract (the "Responsible Manager").

(A) The managing venturer is responsible for controlling the day-to-day management and administration of the contractual performance of the joint venture, but other partners to the joint venture may participate in all corporate governance activities and decisions of the joint venture as is commercially customary. The joint venture agreement may not give to a non-managing venturer negative control over activities of the joint venture, unless those provisions would otherwise be commercially customary for a joint venture agreement for a government contract outside of SBA's programs. A non-managing venturer's approval may be required in, among other things, determining what contract opportunities the joint venture should seek and initiating litigation on behalf of the joint venture.

(B) The individual identified as the Responsible Manager of the joint venture need not be an employee of the small business at the time the joint venture submits an offer, but, if he or she is not, there must be a signed letter of intent that the individual commits to be employed by the small business if the joint venture is the successful offeror. The individual identified as the Responsible Manager cannot be employed by the mentor and become an employee of the small business for purposes of performance under the joint venture.

Organization Conflicts of Interest

© 2025 Fox Rothschild LLP

DirectViz Solutions, LLC, B-423366 et al.

Key Legal Issue

What is the blueprint for assessing and protesting organizational conflicts of interest?

An Organizational Conflict of Interest (OCI) in government contracting arises when a contractor's ability to perform work impartially and in the best interest of the government is potentially compromised due to its relationships, roles, or access to information. OCIs typically occur in three main scenarios:

- **Impaired Objectivity:** When a contractor is in a position to evaluate its own products or services, or those of a competitor, which may bias its judgment.
- **Unequal Access to Information:** When a contractor has access to non-public, proprietary, or sensitive information that could provide an unfair competitive advantage in future procurements.
- **Biased Ground Rules:** When a contractor helps set the terms, specifications, or requirements for a contract in a way that could favor itself in the bidding process.

DirectViz Solutions, LLC, B-423366 et al.

Overview of the Protest and OCI Issue

- DirectViz Solutions protested the Army's award of a cybersecurity support services task order to Peraton, Inc., alleging, among other things, that Peraton had unmitigated OCI due to its performance on a related Army Cyber Command task order.
- The protest focused on whether Peraton's concurrent roles under both the task orders created an "impaired objectivity" OCI.

DirectViz Solutions, LLC, B-423366 et al.

GAO's Holding

- GAO sustained the protest on the basis that the Army's OCI analysis was unreasonable and insufficient.
- GAO recommended that the Army conduct a new, meaningful OCI analysis, and, if an OCI is found, take appropriate steps to avoid, neutralize, or mitigate the conflict, or consider a waiver.

OCI Comparison

Lockheed Martin Corporation, B-423294 (May 02, 2025)

- The protest hinged on the existence of alleged unmitigated OCI based on the awardee's concurrent role as the software integrator for the Air Force's Cloud-Based Command and Control (CBC2) program. That is, the protest argued that the awardee's involvement in both programs resulted in impaired objectivity and unequal access to information.
- GAO denied the protest, concluding that the Air Force reasonably assessed and approved the actions taken by the contractor and the agency to identify and mitigate the OCI.

Cybersecurity and Enforcement

© 2025 Fox Rothschild LLP

United States et al. v. MORSECORP Inc. et al., No. 1:23-cv-10130 (D. Mass.)

Landmark enforcement action under the False Claims Act (FCA) for cybersecurity noncompliance by a federal defense contractor. MORSECORP Inc. (MORSE), a Massachusetts-based defense contractor, agreed to pay $4.6 million to resolve allegations that it failed to comply with mandatory cybersecurity requirements in its contracts with the U.S. Army and Air Force.

United States et al. v. MORSECORP Inc. et al., No. 1:23-cv-10130 (D. Mass.)

- **Third-Party Cloud Security**: From January 2018 to September 2022, MORSE used a third-party email hosting provider without ensuring the provider met the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline, as required by Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.
- **Incomplete Implementation of NIST SP 800-171 Controls**: Between January 2018 and February 2023, MORSE failed to fully implement the cybersecurity controls required by NIST Special Publication 800-171, which are designed to protect Controlled Unclassified Information (CUI).
- **Lack of System Security Plans**: From January 2018 to January 2021, MORSE did not maintain a consolidated written system security plan (SSP) for its covered information systems, as required by contract.
- **False and Inaccurate Reporting**: In January 2021, MORSE submitted a highly favorable cybersecurity compliance score (104 out of a possible 110) to the Department of Defense's Supplier Performance Risk System (SPRS). However, a third-party assessment in July 2022 found the actual score to be -142, indicating severe noncompliance. MORSE did not update its SPRS score until June 2023, after being served with a government subpoena.

United States et al. v. MORSECORP Inc. et al., No. 1:23-cv-10130 (D. Mass.) cont.

- **First-of-its-Kind Enforcement**: This is the first FCA settlement based on a contractor's failure to update its SPRS score after a third-party assessment revealed significant noncompliance.
- **DOJ's Civil Cyber-Fraud Initiative**: The case is part of the Department of Justice's broader effort to use the FCA to enforce cybersecurity requirements in federal contracting, signaling increased scrutiny and risk for contractors who misrepresent their cybersecurity posture.
- **Whistleblower Role**: The case underscores the importance of internal reporting and the powerful incentives for whistleblowers to report cybersecurity noncompliance.

Looking Ahead to 2026

- Anticipate Heightened Scrutiny and Enforcement (in certain areas)
- Focus on Strengthening Cybersecurity
- Bidding and Protest Best Practices
- Innovation

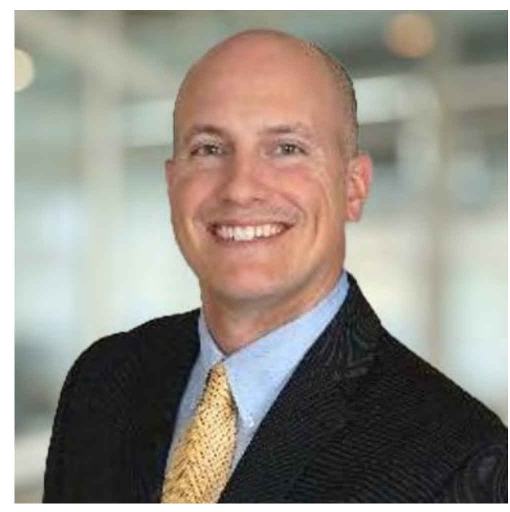
Thank you!

Nick Solosky
Partner, Fox Rothschild

202.696.1460
nsolosky.@foxrothschild.com

Michael Vozzo
Senior Director of Litigation Management and Strategy, Constellis

315.395.6832
mike.vozzo@constellis.com



Michael Bauer
General Counsel, Versar, Inc.

202.984.0338
MBauer@versar.com

© 2024 Fox Rothschild LLP

Thank you!

Fox Rothschild forvis mazars Marsh

© 2025 Fox Rothschild LLP

Bid Protests in an Era of Consolidated Procurements

Panelists:

- Brenna Duncan, Senior Counsel, Bechtel National, Inc.
- Meg Nielsen, General Counsel, Combat and Trainer Engines, GE Aerospace
- Lauren Schlanger, Deputy Chief Counsel, BAE Systems OSI

Moderators:

- Luke Levasseur, Partner, Fox Rothschild
- Evan Williams, Partner, Fox Rothschild

© 2025 Fox Rothschild LLP

Summary

- Emerging bid protest issues
  - The push for consolidated procurements and impact on protests
  - GAO's report to Congress responding to FY2025 NDAA section 885 and related protest trends
- Notable protest litigation trends and cases
  - GAO's revised protest pleading standard
  - Recent case on standing – *Precipient.ai (Fed. Cir. Aug. 28, 2025)*
  - Use of artificial intelligence in protest litigation

Protests in a Time of Consolidated Procurements

- Background
  - o Long line of statutes designed to increase acquisitions of commercial products and services
  - o Federal government has taken recent steps to increase speed and efficiency in government contracting
- General Services Administration (GSA)
  - o Executive Order 14240 (March 2025)
    - ▪ Directs agencies to shift the purchasing of common products and services to the GSA
  - o GSA's June release of the final version of its legislative proposal to support the consolidation
  - o Revolutionary Federal Acquisition Regulation Overhaul (RFO)
  - o Agencies will be required to use existing GSA or government-wide contracts before creating new ones, unless justified
  - o Goal is to expand use of "best-in-class" contracts to leverage government's collective purchasing power and reduce administrative costs

Protests in a Time of Consolidated Procurements, *cont'd*

- Other Recent Developments
  - EO 14271, April 2025: Requiring procurement of commercial products and services "to the maximum extent practicable“
  - EO 14265, April 2025: Requiring DOD to prioritize commercially available solutions and use of Other Transaction Authority (OTA)
- Effect on Protests
  - Consolidation means fewer procurements to protest
  - Commercial acquisition procedures are streamlined → harder to effectively challenge
  - Increased use of indefinite delivery/indefinite quantity (IDIQ) contracts
    - Protest thresholds ($10 million for civilian / $35 million for DOD)
  - Limited protest jurisdiction over OTA acquisitions (which are not FAR-based)

Efforts to Reform the GAO's Bid Protest Process and the GAO's Response to FY2025 NDAA Section 885

GAO's Response to Congressional Demand for Bid Protest Analysis and Potential *Reform*

- Congressional and other complaints about purportedly "frivolous" protests at GAO
- The 2018 RAND Report – finding, conclusions
- Section 885 of the FY2025 NDAA indicates Congress still has questions; instructed GAO and DOD to analyze bid protest data and provide:
    - A proposal for an enhanced pleading standard that an interested party – i.e., a protester – could be required to satisfy in its initial filing to pursue a bid protest and to gain access to an agency's administrative record
    - Information regarding potential penalties to be assessed against unsuccessful protester, e.g., benchmarks/ categories of protest-related costs that could be used as penalties (including average cost of DoD-related protests and "lost profit" rates of awardees (whose performance may be delayed by protests)
    - A potential process under which an unsuccessful protester could be required to pay the government and the contract awardee in the event of an unsuccessful protest
- GAO proposed an enhanced pleading standard that we'll discuss next

GAO's Response to Congressional Protest Demands, *cont'd*

- Regarding fee shifting and potential penalties for unsuccessful protesters
  - As addressed in the 2018 RAND Study and explained by GAO in response to 885, GAO and DoD lack the types of data needed to response to Congress' cost or fee-shifting questions or to support such cost/fee shifting
  - GAO explained there was no need for lost fee or lost profits awards, which would cause substantial problems under its mandate and rules
- Bid protests' role in procurement system: only meaningful, timely, potentially effective process to uncover and address violations of procurement law and unreasonable agency actions
- Effectiveness rate raises substantial questions about criticism of protests
- Few "frivolous" protests and GAO has effective means to deal with them
- Examples of problematic protest types can't withstand scrutiny
- Odd timing of congressional questions – recent decline in GAO bid protests
  - 1,740 protests in 2024, which is down 10% from 2023; downward trend since 2015; COFC protests on the rise
- Probable effects of potential cost/fee shifting rule
- Article from *Law360*

GAO's Revision to its Bid Protest Pleading Standard

GAO's Revision to its Protest Pleading Standard

- Reason for the revision?
- GAO's prior "formulation" of its pleading standard:

  Protesters must "provide, at a minimum, either allegations or evidence sufficient, if uncontradicted, to establish the likelihood of the protester's claim of improper agency action."

- Has been changed to:

  Protesters must "provide, at a minimum, ***credible*** allegations ***that are supported by evidence and are*** sufficient, if uncontradicted, to establish the likelihood of the protester's claim of improper agency action."

- Was the language revision a clarification or a substantive change?

Decisions Applying GAO's Revised Pleading Standard

- *Warfighter Focused Logistics*, B-423546, Aug. 5, 2025
  - No evidence for speculative claim that awardee misrepresented its supply
- *Navarre Corporation*, B-423602, Aug. 14, 2025*
  - No evidence for allegation that agency improperly diverted trips to awardee
- *DS Imports*, B-423665, Aug. 20, 2025
  - Allegation did not, on its face, demonstrate improper agency action
- Enviremedial Services, Inc., B-423552, Aug. 28, 2025*
  - "Bare assertions" of price disparities between offerors does not show unbalanced pricing
- Alliant Health Solutions, B-423598, Sept. 12, 2025*
  - Conflict of interest allegation based on factually inaccurate statement

** Protester represented by outside counsel*

Recent Decision: Precipient.ai Standing

Standing – *Precipient.ai* (Fed. Cir.)

- Rare *en banc* decision of the Federal Circuit
- Percipient.ai's protest concerned a previously awarded National Geospatial-Intelligence Agency (NGA) contract for the SAFFIRE program regarding improved collection, interpretation, and storage of visual intelligence, and operation of a repository for data storage and dissemination
- Percipient did not compete for SAFFIRE, which was a single-award IDIQ
  - Percipient wanted to satisfy SAFFIRE's "Computer Vision" (**CV**) requirement with its commercial CV platform but Percipient could not satisfy SAFFIRE's Structured Observation Management Enterprise Repository (**SER**) requirement
  - Percipient didn't propose a solution (or team with another contractor) for SAFFIRE
- The awardee's (CACI) contract incorporated FAR 52.244-6 and required inclusion of commercial or non-developmental items to the maximum extent practicable
- For Task Order 1 (re CV), Percipient tried to interest (and sell to) CACI but got nowhere
- Percipient complained to NGA and got nowhere
- Percipient's protest at COFC was dismissed; its appeal resulted in reversal; but the *en banc* Federal Circuit affirmed, effectively re-instating the COFC dismissal (with a different rationale)

Precipient.ai, *cont'd*

- Federal Circuit provided exhaustive historical explanation of legislation affecting bid protest jurisdiction and standing as well as key judicial decisions
- *Standing test*: Traditionally limited to "actual or prospective bidders or offerors whose direct economic interests would be affected by the award of the contract or by the failure to award the contract"
- 28 USC 1491(b) provides jurisdiction to consider a protest "by an interested party objecting to":
  - "a federal agency's solicitation for bids or proposals for a proposed contract"
  - "or to a proposed award or the award of a contract"
  - "or any alleged violation of statute or regulation in connection with a procurement or a proposed procurement"
- Percipient argued 1491(b) has three "prongs" and that a protester did not have to be an actual or prospective offeror to challenge an "alleged violation of statute or regulation in connection with a procurement or proposed procurement"
- Federal Circuit panel accepted that Percipient's argument
- *En banc* court rejected contention that the definition of "interested party" changed based on the "prong" under which the plaintiff brought its protest

Use of AI in Bid Protest Cases

Use of AI in Protest Litigation

A brave new world? → Potential applications

- Government
  - Evaluation of proposals
  - Source selection / best-value determinations
- Protest counsel
  - Review documents
  - Identify potential protest grounds
  - Legal research
  - Draft briefs
  - Risk assessments / predictive analytics

Use of AI in Protest Litigation, *cont'd*

Benefits?

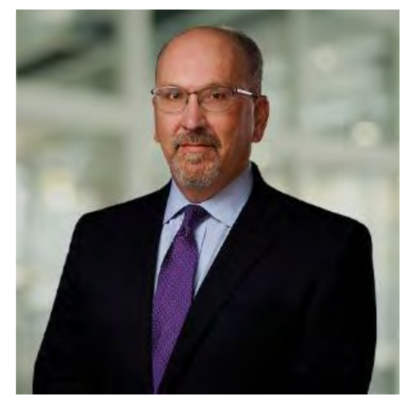
- Increased speed and efficiency
- Improved accuracy -- attention to detail
- Lower costs
- Ability to leverage vast amounts of data

Risks?

- Spillage (e.g., GAO protective orders, attorney-client privilege)
- Hallucination -- *Oready, LLC*, B-423649, Sept. 25, 2025
- Verification of output (associated costs)
- Overestimation of AI abilities/competence
- Malpractice

Remaining questions?

Contacts



Luke Levasseur
Partner

Fox Rothschild
llevasseur@foxrothschild.com

Evan C. Williams
Partner

Fox Rothschild
evanwilliams@foxrothschild.com

© 2024 Fox Rothschild LLP

Thanks to Our Panelists!

Brenna Duncan
Senior Counsel

Bechtel National, Inc.
bduncan@bechtel.us

Meg Nielson
General Counsel

Combat and Trainer Engines, GE Aerospace
margaret.nielsen@geaerospace.com

Lauren Schlanger
Deputy Chief Counsel

BAE Systems OSI
lauren.schlanger@baesystems.us

© 2024 Fox Rothschild LLP

Thank you!

Marsh

© 2025 Fox Rothschild LLP

Developing Strategies for M&A in an Uncertain Market

Panelists:

- Laura Howard, Partner, Fox Rothschild
- Eric Chen, Executive Vice President, Interim General Counsel and Corporate Secretary, Global Infrastructure Solutions Inc
- Susan Gabay, Managing Director, Houlihan Lokey

© 2025 Fox Rothschild LLP

Federal Government Contracting - Market Snapshot and Deal Drivers

- Resilient demand: mission-critical spend (defense, cyber, IT modernization).
- In 2024, there were 105 transactions completed (HL M&A Database).
- In 2025, the number of deals through Q3 is ~60 (Run-rate of ~80; represents 24% decrease YoY).
- Initial freeze after "Liberation Day" has ceded to an uptick in activity as fears abate.
- PEs still constitute majority (60-70%) of transactions, even as they experience challenges exiting existing positions.
- Budget/priorities: "great power" competition, zero-trust, AI adoption, supply chain.
- Buyer mix: strategics consolidating capabilities; active PE platforms/add-ons.
- Rationale: access to contract vehicles, cleared talent, past performance, scale.

What is Being Bought

- Cybersecurity and zero-trust engineering.
- AI/ML, data engineering, model ops for mission analytics.
- Cloud migration.
- Space technology/Communications/Earth Observation Satellites.
- Digital health/VA, CMS, HHS modernization.
- Logistics, supply chain risk, and microelectronics/security.
- Classified intel and special missions (high barriers to entry).

Valuations, Structures, and Diligence Realities

- Valuations: premium for high-growth, tech-forward, strong CPARS (Contractor Performance Assessment Reporting Systems). As always the case, firms whose businesses are primarily with three letter agencies, high % security clearances, etc. command a premium.
- Structures: carve-outs, add-ons; earnouts/retention, seller rollover common.
- Key diligence: pipeline realism, recompete map, OCI (Organizational Conflict of Interest) risks, facility clearances.
- Integration: novation of contracts, TS/SCI (Top Secret/Sensitive Compartmented Information) transition, pricing/cost realism, culture retention.
- Regulatory: antitrust/CFIUS, FOCI (Foreign Ownership, Control or Influence) mitigation, supply chain (EO/DFARS) (Executive Orders and Defense Federal Acquisition Regulation Supplement), cyber (CMMC) (Cybersecurity Maturity Model Certification).

Outlook and How to Prepare (Next 12–24 Months)

- While DOGE-ing of US AID was quite possibly a singular / one-off episode, exercise caution on other potentially disfavored markets.
- Budget uncertainty creates timing windows but not structural demand decline. It is possible that US AID was a singular example.
- Talent scarcity and cleared labor inflation persist; retention is deal-critical.
- Sellers: focus on backlog quality, prime positions, differentiated past performance.
- Buyers: prioritize synergy / duration from contract vehicles, capture leadership, and BD rigor.

Panelists

Laura Howard
Partner

Fox Rothschild
lthoward@foxrothschild.com

Eric Chen
Executive Vice President

Global Infrastructure Solutions Inc.
echen@gisi.com

Susan Gabay
Managing Director

Houlihan Lokey
sgabay@hl.com

© 2024 Fox Rothschild LLP

Thank You!

© 2025 Fox Rothschild LLP

Networking Break

10:30–10:45 a.m.

Revolutionary FAR Overhaul

***Speakers*:**

- Keeley McCarty, Partner – Fox Rothschild LLP
- Bryce Chadwick, General Counsel – Drodex
- Larry Allen, Associate Administrator Governmentwide Policy & Chief Acquisition Officer – GSA

Fox Rothschild forvis mazars Marsh

© 2025 Fox Rothschild LLP

Federal Acquisition Regulation History

- FAR is primary set of regulations that govern procurements by executive agencies
- Armed Services Procurement Regulation (ASPR) enacted in 1948
- Office of Federal Procurement Policy (OFPP) created in 1974 to unify government-wide regulations
  - By 1979, 877 different sets of procurement regulations existed across 19 agencies
- OFPP established the first iteration of the FAR in 1984

CICA, FASA & FARA: Modern Competitive Procurement

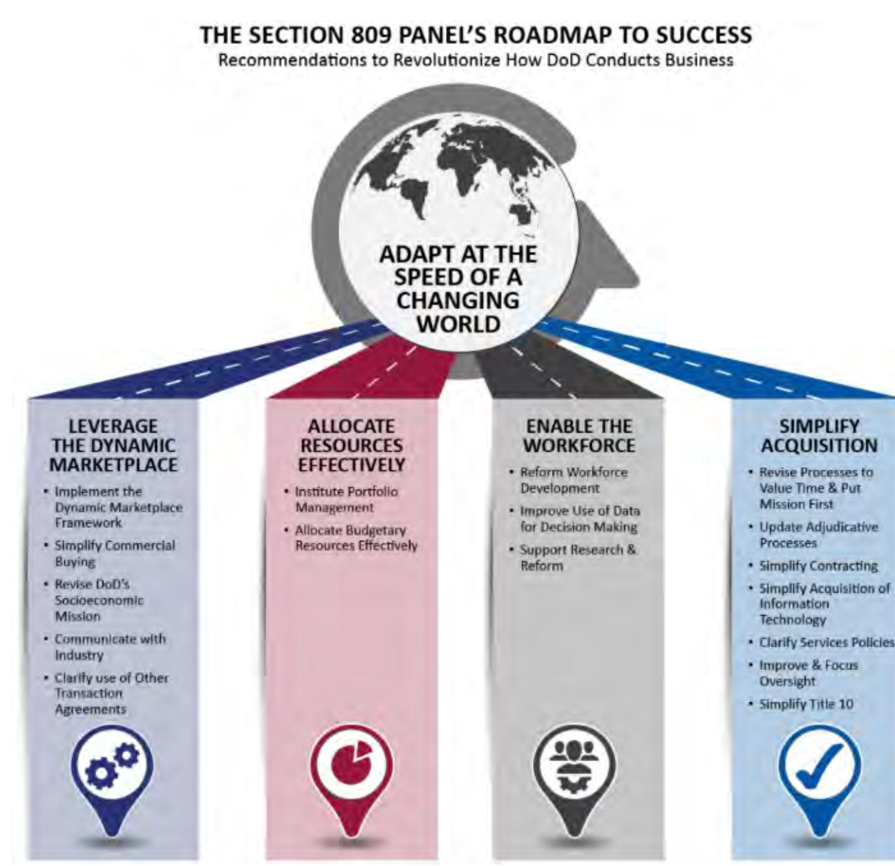
1984: Competition in Contracting Act (CICA) – promoted full and open competition

1994: Federal Acquisition Streamlining Act (FASA) – encouraged commercial item acquisition

1996: Federal Acquisition Reform Act (FARA)

Section 809 Panel: A Modern Reform Blueprint

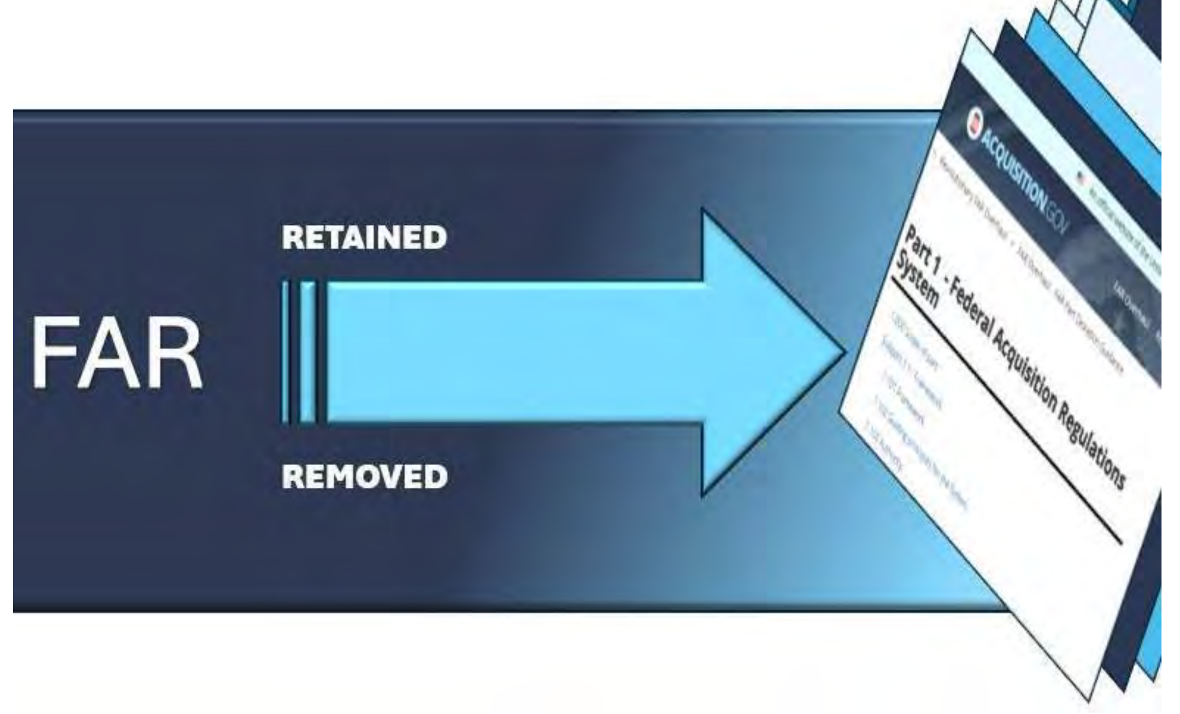
- Established by FY 2016 National Defense Authorization Act
- Recommended Dynamic Marketplace Framework for DoD
- Proposed eliminating outdated statutes and improving acquisition agility



Revolutionary FAR Overhaul: The Origin

- **EO 14271-Ensuring Commercial, Cost-Effective Solutions in Federal Contracts (April 15)**
  - Seeks to shift federal procurement to "suitable or superior" commercial solutions instead of "custom products and services"
  - Claims agencies spent too much procuring custom goods and services and evading FASA preference for commercial goods and services
- **EO 14275-Restoring Common Sense to Federal Procurement (April 15)**
  - Seeks to create agile, effective, and efficient procurement by removing "unnecessary" and non-statutory acquisition rules at all levels
  - Endeavors to improve access to federal contracting, especially for small and new businesses
  - Calls for action to be taken within 180 days (by October 12, 2025)

Revolutionary FAR Overhaul: The Goals



- Remove non-statutory requirements
- Enable commercial-like, agile procurements
- Increase competition
- Shorten FAR to a manageable size
- Reword using plain language

RFO Rollout Process

- Phase 1: FAR Council issues deviations that must be adopted by each agency to take effect
  - "Agencies ***should*** generally issue individual or class deviations to implement the FAR Council's deregulated coverage within 30 days after the model deviation text is released." OMB Memo M-25-26
- Phase 2: Formal notice & comment rulemaking
  - 41 U.S.C. § 1707 procedures
  - Will incorporate public feedback on deviations

Revolutionary FAR Overhaul: The Status

- All parts released as of September 30
- Several parts released as PDFs without accompanying Practitioners Album
  - Part 22 – Application of Labor Laws to Government Acquisitions
  - Part 23 – Sustainable Acquisition, Material Safety, and Pollution Prevention
  - Part 32 – Contract Financing
  - Part 53 – Forms
- FAR Companion Guide v1 released
- Varying adoption by agencies

What’s so Revolutionary?

- Plain language & structural overhaul
- Automatic sunsets
- Digital oversight and transparency
- Mandatory “best-in-class” contracts
- FSS ordering procedures moved
- 1000 shalls and musts removed

FAR Part 6 – Competition Requirements

- Overview
  - Revised to be more concise and straightforward; few substantive changes
  - Competition requirements largely derive from the Competition in Contracting Act of 1984 (CICA)
- Highlights
  - Simplified documentation requirements for sole-source justifications
  - Removes certain small business set-aside requirements → FAR 19

FAR Part 8 – Required Sources of Supplies & Services

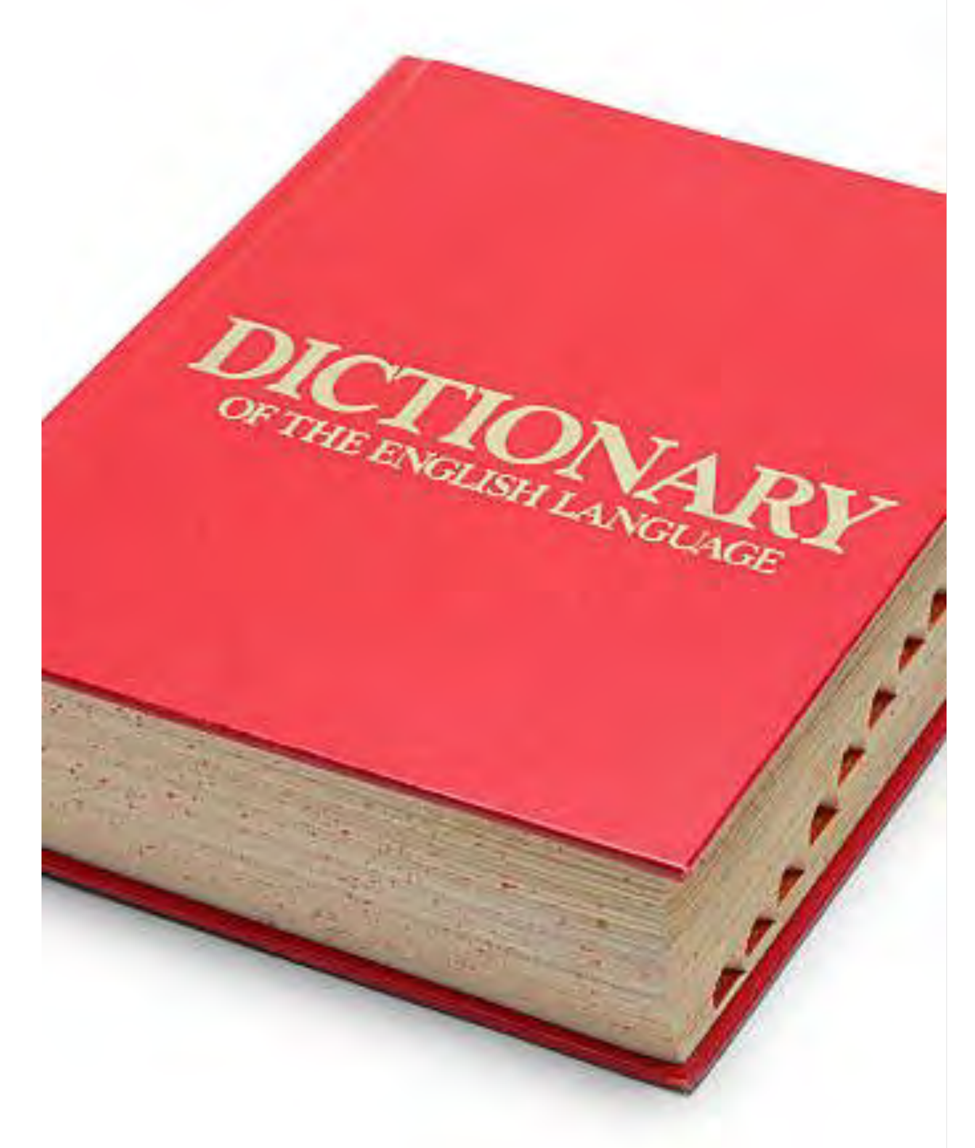
- Moves FSS ordering procedures to GSAR
- Establishes government-wide "required use" contracts or BPAs that must be used when a commercial product or commercial service meets an agency's need
  - OFPP to issued guidance on what vehicles are "required use" contracts
- Distinguishes between quotations and offers
  - No requirement for evaluation plans, quotation scoring, or competitive range before communicating with quoters or soliciting revised quotations
- Increased contractor access to government supply sources

FAR Part 12 – Acquisition of Commercial Products and Commercial Services

- Incorporates the *Simplified Acquisition Procedures* from FAR Part 13
  - Mandates use of simplified procedures for acquisitions under $7.5 million
  - Procurements above $7.5 must use either procedures for request for proposals (FAR Part 15) or invitation for bids (FAR Part 14)
- Defines "commercial service" to include construction
- Eliminates roughly 30% of applicable provisions and clauses
  - Deletes FAR 52.212-3 & FAR 52.212-5
- Major change to FAR 52.212-1's "Late is Late" rule
  - Revised to allow acceptance if late offer is received before award and will not unduly delay acquisition

FAR Part 15 – Contracting by Negotiation

- Discussions → Negotiations
- Clarifications include what used to be Communications
  - Still cannot use to cure proposal deficiencies
  - Can conduct clarifications from receipt of proposals through contract award
- Deficiency no longer includes combination of significant weaknesses
  - Defines material requirement of RFP as one that affects price, quantity, quality, or delivery, or that RFP requires to be met at time of proposal
- Proposal revision limited to change to material elements of proposal



FAR Part 15 – Contracting by Negotiation

- Contracting officer determines the competitive range based on those proposals "best suited for further negotiation" rather than most highly rated
- Two new evaluation approaches
  - FAR 15.103-3 Highest Technically Rated with Fair & Reasonable Price
    - Appropriate when the government determines in advance that it would not be advantageous to consider tradeoffs
  - FAR 15.103-4 Phased Acquisitions
    - Separate awards at distinct phases of the acquisition
    - Promotes flexibility by permitting adjustments to the requirement between phases
- Six subparts reduced to five

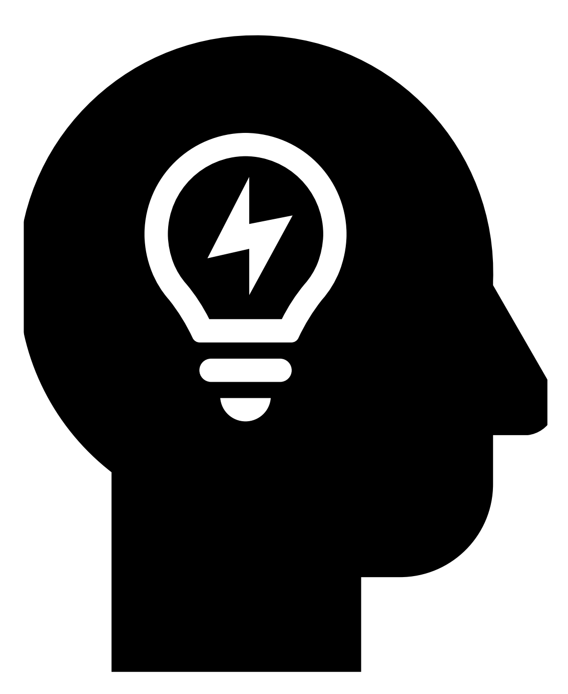
FAR Part 19 – Small Business (Programs)

- Retains Rule of 2 above the micro-purchase threshold and above the simplified acquisition threshold
  - Only applies to contracts, not task orders
  - COs have discretion to set aside IDIQ task orders; not a basis for protest
- Eliminates size recertification for task order awards
  - Size is determined at contract award, novation, options
  - 13 C.F.R. § 125.12(c) still allows COs to request recertification for orders
- For acquisitions below the competitive threshold, COs must attempt competitive 8(a) order before awarding sole-source
- 8(a) follow-ons can be automatically released for set aside to HUBZone, SDVOSB or WOSB programs

FAR Part 36 - Construction & Architect-Engineer Contracts

- Reorganized into 3 Phases: Pre-Solicitation, Evaluation & Award, and Postaward
- Removes FAR 36.501 (Performance of Work by the Contractor) and FAR 52.236-1 (Performance of Work by the Contractor) (the "12% rule")
  - Note: This is separate from 52.219-14 (Limitations on Subcontracting)[for Set-Asides]
- Eliminates 36.602-1 Selection Criteria for A/E Contracts
- Project Labor Agreement requirement for projects ≥ $35M maintained
- Enhances rules for two-phase design-build
- Deletes definitions of "Design-Bid-Build" and "Design-Build" from FAR subpart 36.102
- Retains FAR subpart 36.209 (Construction Contracts with Architect-Engineer Firms) as new 36.201-1 Limitations
  - "The CO must not award a contract for construction – (b) To the firm that designed the project or the firm's subsidiaries or affiliates, unless approved by the agency head."
- Embeds required FAR Part 52 Clauses directly into Part 36

Other Highlights



- Part 13 – now focused on acquisitions below SAT
- Part 16 – BPAs now permitted under multiple-award contracts
- Part 25 - nonavailability determinations centralized at the Made in America Office (MIAO)
- Part 42 – past performance info can be used outside of source selection

Launch of the RFO Website

- Acquisition.gov/far-overhaul
- Live as of May 6, 2025
- Central hub for deviations, Practitioner Albums, and feedback:
  - Shows which agencies have adopted deviations
  - Practitioner Album provides redline of old FAR
  - Includes FAQ

Quick Access to Key RF

PARTS AND DEVIATIONS

Access the definitive list of overhauled

FAR COMPANION

FAR COMPANION FEEDBACK

Access the FAR Companion, a living

PRACTITIONER ALBUMS

Explore non-regulatory training m
out documents highlighting remov

FREQUENTLY ASKED QUESTIONS

Choose from a list of frequently asked qu

© 2025 Fox Rothschild LLP

OMB Legislative Proposals for RFO

- Increase Simplified Acquisition Threshold for commercial products and services from $250,000 to $10 million over 5 years
- Increase the Micro-Purchase Threshold from $10,000 to $100,000 over 5 years
- Grant GSA and DHS permanent Commercial Solutions Openings (CSO) authority, and NASA new CSO authority
- Increase task order protest threshold from $10 million to $35 million for civilian agencies
- Raise the CAS threshold from $2 million to $35 million
- Repeal executive compensation reporting

Questions?

Marsh

© 2025 Fox Rothschild LLP

Contact

Keeley McCarty

Partner, Fox Rothschild

202.461.3101
Kmccarty@foxrothschild.com

Bryce Chadwick

General Counsel, Drodex

bchadwick@drodex.com

Larry Allen

Associate Administrator Governmentwide Policy & Chief Acquisition Officer, GSA

larry.allen@gsa.gov

© 2024 Fox Rothschild LLP

Networking Lunch

11:45–12:30 p.m.

Effective Corporate Compliance Programs in an Evolving Enforcement Landscape

Speakers:

- Diana Lyn Curtis Shutzer, Fox Rothschild LLP
- Olivia Fines, Chief Legal Risk & Compliance Officer, Constellis, LLC
- Erica Roumieu, Deputy General Counsel, Versar, Inc.

Fox Rothschild forvis mazars Marsh

© 2025 Fox Rothschild LLP

Objectives

- Understand 2025 enforcement shifts affecting contractors
- Key executive orders and DOJ guidance
- DOJ's current focus area and recent settlements
- Voluntary self-disclosure decisions under new policies
- Practical action plan and checklist

Big Picture: Why This Matters Now

- Post-election policy shifts
- Evolving DOJ priorities
- EO 13,209 pausing FCPA enforcement
- Recession of EO 13,989 (Ethics Commitments by Executive Branch)
- DOJ memos re-focusing on harm to U.S. interests and national security
- Conclusion: Compliance is not optional. Stay the course.

Stay the Course On Compliance

- FCPA pause is temporary
- Statutes of limitations (5-6+ years) - today's conduct remains exposed
- Strong programs attract customers, investors, partners, and employees
- Focus on fraud, waste, abuse → expect clawbacks

E0 14,209: FCPA Pause (February 19, 2025)

- Halts ongoing/new FCPA actions for 6 months; extendable to February 2026
- Directs AG to revise guidance to prioritize U.S. interests and resource efficiency
- DOJ to prioritize cases with "specific and identifiable" harm to U.S. companies/individuals
- Heightened focus on cartels and transnational criminal organizations
- De-emphasis on de minimis business courtesies
- Emphasis on substantial bribes

FCPA Pause: Practical Implications

- FCPA Statute Intact: Books/records, internal controls still required
- Statute of Limitations: 5 years (antibribery), 6 years (accounting)
- Foreign evidence may extend
- Other regimes still apply: UK Bribery Act and FEPA (criminalizes demand side)
- SEC has not formally abandoned FEPA as a priority and EO 14,215 seeks alignment

EO 14,148: Rescinding EO 13,989 (Ethics Pledge)

- Ethics pledge: Rescinded
- Minimal legal impact for contractors
- Ongoing laws still govern: LDA (registration/reporting), 18 U.S.C § 201 (bribery), state bribery laws
- Practical takeaway: Keep existing ethics/lobbying compliance practices

EO 14,215: Ensuring Accountability for All Agencies

- Seeks alignment of independent agencies (e.g., SEC) with Presidential/AG legal positions
- Unknown extent of SEC adjustment on FCPA and related priorities

DOJ’s White-Collar Focus

- Priority areas:
  - Health care fraud
  - Procurement fraud
  - Trade/customs (tariff evasion)
  - Offenses tied to Chinese-owned companies
  - Financial fraud
  - Bribery
- Policy aim: Focus, fairness, efficiency. Avoid overbroad burdens.

Evaluation of Corporate Compliance Programs DOJ Update: What Prosecutors Ask

- The ECCP guidance is centered around three questions:
  - Is the corporation's compliance program well-designed?
  - Is the program being applied earnestly and in good faith?
  - Does the corporation's compliance program work in practice?
- New focus:
  - Emerging Tech/AI: Assess risks, controls policies
  - Data Access: Provide compliance meaningful data/analytics
  - Whistleblowers: Protections and incentives

Enforcement Continues: FCA Clawbacks

- FY 2024: $2.9B in FCA settlements/judgments
- Emphasis on fraud, waste, abuse → expect continued enforcement
- Implication: Internal controls and documentation are critical

Case Study: Cybersecurity Enforcement

- CMMC 2.0 final; DFARS 252.204-7008/7012; NIST SP 800-171
- DoD assessment score posting to SPRS required (-203 to 110)
- $4.6M FCA settlement: Noncompliant cloud email; missing required controls; missing plans for covered systems; reported 104 but third-party assessed -142; delayed score update until probe
- Lessons:
  - Validate third-party vendors/cloud against DFARS/NIST
  - Keep SRS scores accurate and updated
  - Maintain written plans and remediation

Case Study: Small Business Eligibility

- $1.3M settlement (Whitcraft): Affiliation after private equity acquisition; 71 small-business set-aside contracts over ~5 years
- Self-detected and self-disclosed → cooperation credit
- Lessons:
  - Monitor size/affiliation status post-transaction
  - Ongoing eligibility checks; correct ASAP and consider disclosure

Immigration Enforcement Focus (Early 2025)

- DOJ memos: Use all available criminal statutes; support DHS removal initiatives
- Target: Resisting/obstructing/failing to comply with lawful immigration-related commands/requests
- Contractor actions:
  - Review hiring (I-9/E-Verify), recordkeeping, cooperation protocols
  - Train managers on responding to lawful requests

DOJ Corporate Enforcement and Voluntary Self-Disclosure Policy

- Non-prosecution if:
  - The company voluntarily self-disclosed the misconduct
  - The company fully cooperated with the DOJ's investigation
  - The company timely and appropriately remediated the misconduct
  - There are no aggravating circumstances.
- Additional benefits even if criteria not fully met

Disclosing During an FCPA Pause?

- Pros:
  - Preserve CEP benefits; preempt whistleblower risk
  - Demonstrate strong controls; reduce penalties is priorities shift
- Cons:
  - Current focus on certain FCPA cases
- Bottom Line:
  - FCPA remains law; SOL extends beyond current term.
  - Silence risks losing disclosure benefits and worsened outcomes later

Corporate Whistleblower Awards Pilot Program

- Violations by financial institutions, including schemes involving money laundering, anti-money laundering compliance violations, registration of money transmitting businesses, and fraud statutes, and fraud against or non-compliance with financial institution regulators
- Violations related to foreign corruption, bribery, kickbacks
- Health care fraud schemes involving private insurance plans
- Violations by or through companies related to trade, tariff, and customs fraud
- Violations by or through companies related to federal immigration law
- Violations by or through companies related to sanctions offenses, material support of terrorism, or cartels and transnational criminal organizations including money laundering, narcotics, Controlled Substances Act, and other violations

Corporate Whistleblower Awards Pilot Program

- Must provide original information (derived from the individual's independent knowledge or analysis)
- Must be voluntary
- Must provide truthful and complete information
- Full cooperation with DOJ's investigation
- Lead to successful forfeiture of $1M

Corporate Whistleblower Awards Pilot Program

- Award Amount:
  - An award of up to 30% of the first $100 million in net proceeds forfeited
  - An award of up to 5% of any net proceeds forfeited between $100 million and $500 million
  - No award on net proceeds forfeited above $500 million
- Implications:
  - Strengthen internal reporting channels and anti-retaliation
  - Accelerate triage to prevent external reporting by insiders

Decision Framework for Self-Disclosure

- Triage:
  - Credible Evidence? Materiality to government/customer
  - Mandatory vs. voluntary (e.g., FAR 52.203-13)
- Investigate promptly, preserve evidence, maintain privilege
- Remediation plan, discipline, and control enhancements
- Board/committee oversight and documentation
- Disclose early to maximize CEP benefits

Priority Compliance Areas: Checklist

- Anti-corruption:
  - Books/records
  - Internal controls
  - Third-party due diligence
  - Gifts/hospitality controls
- Cybersecurity:
  - DFARS/NIST conformance
  - CMMC readiness
  - SPRS accuracy
  - Vendor oversight

Priority Compliance Areas: Checklist (cont.)

- Small business/eligibility
  - Size/affiliation monitoring
  - Certification accuracy
  - Transaction diligence
- Immigration:
  - I-9/E-Verify
  - Response protocols
  - Training

Priority Compliance Areas: Checklist (cont.)

- Data/AI governance:
  - Risk assessments
  - Guardrails
  - Compliance access to data
- Whistleblowers:
  - Policies and training
  - Non-retaliation prompt intake/investigation
- Training/Monitoring:
  - Role-based, periodic testing
  - Analytics-driven monitoring

Data and AI in Compliance

- Ensure compliance has access to operational data and analytics
- Align compliance tech resources with business use of data (reasonable party)
- AI:
  - Policy for acceptable use, bias/accuracy and controls auditability
  - Compliance at the table for system selection and deployment

90-Day Action Plan

- Inventory contracts and regulatory obligations (DFARS/FAR; CMMC; SBA; immigration)
- Quick gap assessments: Cyber (NIST controls, SPRS) anti-corruption, size status
- Validate third-party/vendor compliance (cloud/email, subs)
- Refresh training: Anti-corruption, cyber hygiene, immigration response, whistleblower
- Tabletop exercises: Incident response and disclosure decision playbook
- Board brief: New CEP/whistleblower program; disclosure authority and threshold

Key Takeaways

- Enforcement priorities shifted
- FCA, cyber, small business, and immigration are active risk zones
- DOJ, CEP, and whistleblower program heighten self-disclosure calculus
- Maintain and document effective, data-enabled compliance programs
- Don't "bet the company" on political winds - base decisions on facts and policy

Contact

Diana Lyn Curtis Shutzer
Partner, Fox Rothschild

202.794.1208
dshutzer@foxrothschild.com

Olivia Fines
Chief Legal Risk & Compliance Officer, Constellis, LLC

703.397.3368
olivia.fines@constellis.com

Erica Roumieu
Deputy General Counsel, Versar, Inc.

202.984.0340
Erica.Roumieu@versar.com

© 2024 Fox Rothschild LLP

Thank you!

Marsh

© 2025 Fox Rothschild LLP

Navigating Federal Anti-Discrimination Laws Under the Trump Administration

***Speakers*:**

- Robbie Pratt, Partner – Fox Rothschild LLP
- Jasmine Anderson, Partner – Fox Rothschild LLP
- Mike Childers, Senior Corporate Counsel – Amazon

Presentation Prepared With the Assistance of:

- Jaeho Lee, Associate – Fox Rothschild LLP
- Nick Feldstern, Associate – Fox Rothschild LLP

© 2025 Fox Rothschild LLP

Anti-Discrimination Executive Orders

- EO 14151 – "Ending Radical and Wasteful Government DEI Programs and Preferencing"
  - **Termination**: Terminates all government "DEI" initiatives, mandates that agencies report anyone (contractors, employees, grantees) who work in DEI/provide DEI programming to the Government, and terminates all equity-related grants and contracts.
- EO 14173 – "Ending Illegal Discrimination and Restoring Merit-Based Opportunity"
  - **Certification**: Directive to add new contract clause to certify compliance with federal anti-discrimination laws and that the contractor does not operate DEI programs that violate those laws. Also adds a contract clause seeking contractor agreement that a violation of federal anti-discrimination law is material under the civil False Claims Act.
  - **Enforcement Threat**: Authorizes DOJ to investigate and report on private sector DEI initiatives and strategize means of deterring private sector DEI programs.
  - **Revokes EO 11246**: Includes equal opportunity/affirmative action requirements for federal contractors for women and minorities.
- Agencies have begun changing policies and terminating/amending contracts to implement these EOs.

Anti-Discrimination Executive Orders (Cont.)

- EO 14168 – "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government"
  - **Policy Change**: Withdraws federal recognition of transgender individuals and orders that no grant funds be used to "promote gender ideology."
  - **Definition Enforcement**: Orders all agencies to enforce laws governing sex-based rights and define gender as "male" or "female."
- EO 14201 – "Keeping Men Out of Women's Sports"
  - **Expansion of Impact**: Threatens revocation of federal funds from any educational institution that allows transgender women to play on women sports teams.

Anti-Discrimination Executive Orders (Cont.)

- EO 14281 – “Restoring Equality of Opportunity and Meritocracy”
  - **Disparate Impact Liability**: Orders agencies to “deprioritize” enforcing statutes and regulations imposing disparate impact liability. This includes EEOC enforcement of disparate impact claims under Title VII of the Civil Rights Act.
- EO 14332 – “Improving Oversight of Federal Grantmaking”
  - **Overhaul of Existing Grants**: Directs an overhaul of the existing regulatory structure and calls for new grant review process.
  - **Grants to Align With Agency Priorities**: Calls for all grants to align with the Administration’s agenda. The categories of grants that don’t align include “racial preferences or other forms of racial discrimination by the grant recipient, including activities where race or intentional proxies for race will be used as a selection criteria for employment or program participation.”

EEOC Policy on Workplace Discrimination

- Under Title VII, ""DEI initiatives, policies, programs, or practices ***may be*** unlawful if they involve an employer or other covered entity taking an employment action motivated—in whole or in part—by an employee's or applicant's race, sex, or another protected characteristic."
- Areas where "DEI-related disparate treatment" can lead to discrimination include hiring and firing, promotion and demotion, and compensation and fringe benefits.
- Providing certain groups access to opportunities can be a cause for discrimination:
  - Training (e.g., "leadership development programs")
  - Mentoring, sponsorship, or workplace networking
  - Internships (e.g., "fellowships" and "summer associate" programs)
  - Selection for interviews
  - Job duties or work assignments

EEOC Policy on Workplace Discrimination Cont

- Workplace groups such as Employee Resource Groups (ERG) and other affinity groups can constitute unlawful segregation. Based on OPM guidance, to be permissible, the group (1) must be open to all employees wanting to participate, (2) cannot provide any special opportunities (training, promotion, etc.) not available to all employees, and (3) the company must give any kind of affinity group the opportunity to form.

OFCCP Policy on Workplace Discrimination

- **Investigations after EO 14151/14173**: OFCCP has paused investigations regarding affirmative action compliance as authorized under the now-revoked EO 11246.
  - **June 27, 2025**: OFCCP invites federal contractors to voluntarily disclose steps they've taken to implement EO 14173 and how they've wound down compliance with EO 11246.
- **Order 08-2025**: Makes clear that OFCCP still enforces the affirmative action requirements of Section 503 of Rehabilitation Act (disabled individuals) and VEVRAA (qualified categories of veterans).*
- *Note: DOL FY 2026 budget proposal eliminates OFCCP and shifts VEVRA oversight to Veterans' Employment and Training Services and Section 503 oversight to EEOC.

Department of Justice Memorandum for All Federal Agencies: "Guidance for Recipients of Federal Funding Regarding Unlawful Discrimination"

- Practices and policies the Administration considers unlawful:
  - Segregation of programs, activities, or resources based on protected characteristics
  - Unlawful use of protected characteristics in hiring and contracting
  - Preferential treatment based on protected characteristics
  - Failure to maintain sex-separated bathrooms
  - Training programs that promote discrimination or hostile environments
  - Use of proxies for consideration of protected characteristics
- **OMB Memo M-25-33 (9/12/2025)**: Directs agencies to abide by the DOJ Memo.
- **DOJ Civil Rights Fraud Initiative**: Using FCA to pursue claims against anyone utilizing DEI to engage in "racist preferences." Encourages qui tam actions by employees or former employees.

DOJ's "Recommendations on Best Practices"

1. Ensure inclusive access
2. Focus on skills and qualifications
3. Prohibit demographic-driven criteria
4. Document legitimate rationales
5. Scrutinize neutral criteria for proxy effects
6. Eliminate diversity quotas
7. Avoid exclusionary training programs
8. Include nondiscrimination clauses in contracts to third parties and monitor compliance
9. Establish clear anti-retaliation procedures and create safe reporting mechanisms

DOJ Memo: Takeaways for Federal Contractors

- While the memo may not be directed at federal contractors, it signals the Administration's statutory interpretation and enforcement priorities.
- DOJ's position is in tension with current socioeconomic small business preferences.
- Federal assistance recipients should review their hiring and contracting practices, training programs, and DEI policies.

Current Litigation

- Several federal cases pending related to the executive orders:
  - *National Association of Diversity Officers in Higher Education (NADOHE) v. Trump*
  - *Chicago Women in Trade (CWIT) v. Trump*
- Cases are currently ongoing, and status could change at any moment.

What Is Not Allowed/Presents a Risk to My Company?

The following items are prohibited:

1. **Affirmative Action Plans and Programs**: Can't base recruiting, hiring, compensation, or promotion on protected characteristics (exception for under Rehabilitation Act and VEVRAA).
2. **Exclusive ERGs**: Cannot provide resources (meeting space, financial support) to ERGs that provide special employment-related opportunities, exclude participation outside protected class, or operate at exclusion of other affinity groups/ERGs.
3. **Other Discrimination**: Cannot otherwise discriminate against employees or potential employees based on protected characteristics.

- Other activities that present risk (but are not necessarily illegal):

1. **Participation in Community Affinity or Workforce Groups**: Groups that represent workforce subset based on protected characteristics (e.g., Women in Construction).
2. **Non-Discriminatory ERGs**: Even if non-discriminatory, risk exists if using company resources without oversight.
3. **Community Benefit Plans**: Allow construction projects to account for local community's economic and cultural well-being but could draw negative attention.

What is Allowed/Should Be Monitored?

The following are still permissible DEI-related activity:

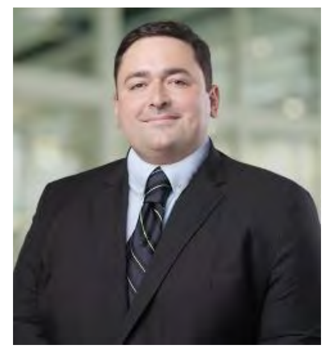
1. **State or Other Diversity Reporting Requirements**: Tracking and reporting characteristics of company workforce is currently not illegal.
2. **Internal or External Messaging or Policies Valuing Inclusion**: The First Amendment protects company statements that it values inclusion and diversity, as long as the company does not use discriminatory practice to foster inclusion.

The following are not prohibited, but should be monitored in light of the changing DEI landscape:

1. **Contracting Preferences**: No formal Administration position on women-owned or historically disadvantaged businesses, the SBA maintains its own preference programs. It is possible the Administration could find this preference is discriminatory.
2. **Transgender-Related Policies**: The Administration has made clear it will not support transgender-related care, funding, or other gender ideology.

Questions?

Contact



Robbie Pratt

Partner

202.696.1453
rpratt@foxrothschild.com

Jasmine Anderson

Partner

418.315.2223
jlanderson@foxrothschild.com

Mike Childers

Senior Corporate Counsel

mikchild@amazon.com

© 2024 Fox Rothschild LLP

Thank you!

Marsh

© 2025 Fox Rothschild LLP

Cost Accounting Standards (CAS) and Fundamentals

Panelists:

- Douglas Hibshman, Partner, Fox Rothschild
- Bill Walter, Partner, Managing Director | GovCon Consulting for Forvis Mazars

© 2025 Fox Rothschild LLP

What is the Purpose of CAS?

- CAS regulations mandate standard practices for measuring, assigning, and allocating **COSTS** to certain federal government contracts
- Covers cost treatment from estimate to contract closeout
- Benefits of CAS:
  - **Government spends lots of money** - $800 billion, many contracts, many agencies
  - **Fair Pricing** due to standardized cost treatment
  - **Contract Management** is easier for both contractor and government due to standardized framework
  - **Government Oversight** is easier due to standardized framework
- **FAR** covers cost allocability, reasonableness, and allowability – Part 31
- **GAAP** covers keeping financial records

What are the Standards?

- BASIC Standards
  - CAS 401: Consistency
  - CAS 402: Direct v. Indirect Costs
  - CAS 405: Unallowable Costs
  - CAS 406: Cost Accounting Period

- The Cost Allocation Standards
  - CAS 407: Standard Costs
  - CAS 414: Cost of Money
  - CAS 410: G&A
  - CAS 403: Home Office expenses
  - CAS 418: Direct & Indirect
  - CAS 420: B&P and IR&D

- Asset Accounting Standards
  - CAS 404: Capitalization
  - CAS 409: Depreciation
  - CAS 417: Self Constructed Assets

- Compensation Standards
  - CAS 408: Compensated Absence
  - CAS 412 & 413: Pensions
  - CAS 415: Deferred Comp

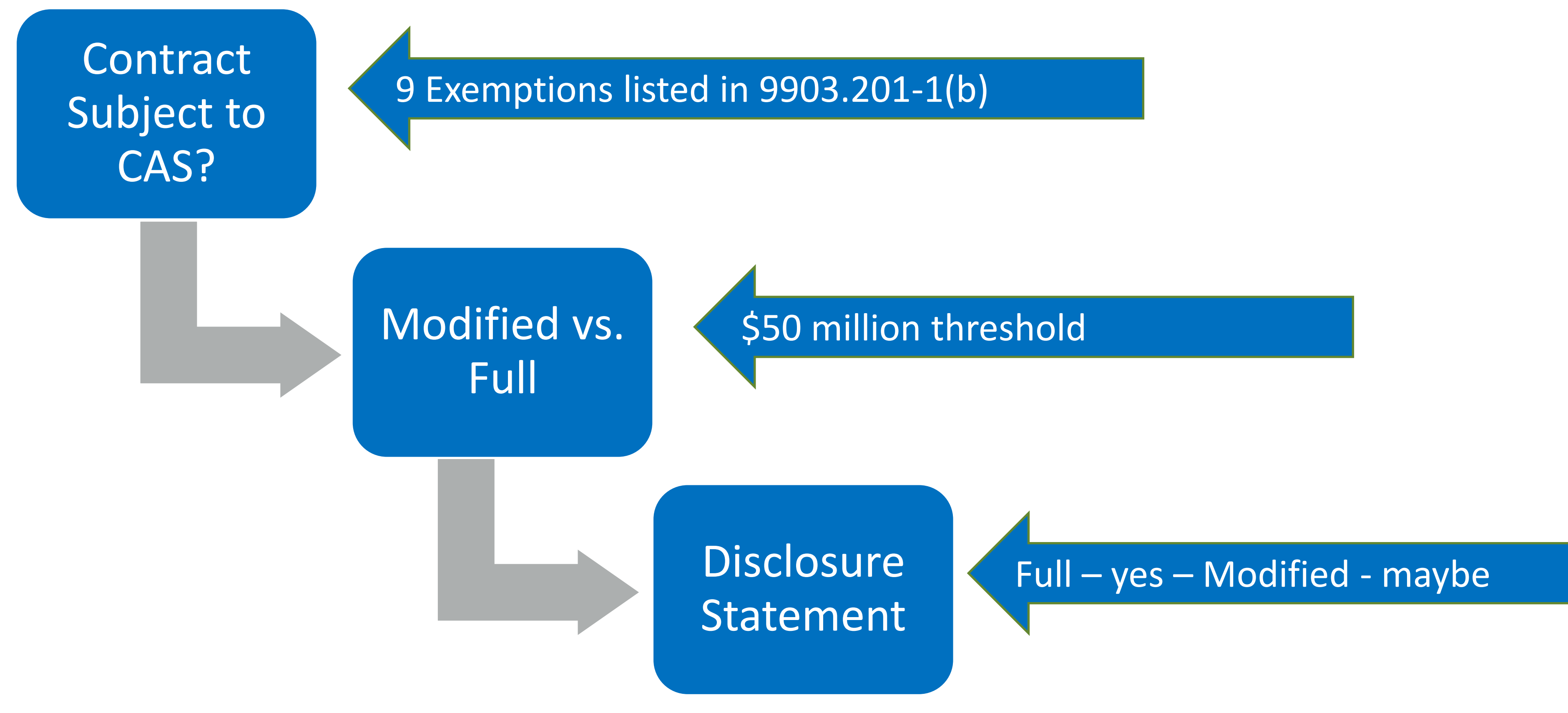
- Other Standards
  - CAS 411: Material Costs
  - CAS 416: Insurance Costs

Who Must Apply CAS?

- Key thread to determine if CAS applies – **COMPETITION OF PRICES**
- CAS Not Required for:
  - FFP contracts / subcontracts based on adequate price competition
  - Sealed bid contracts / subcontracts
  - Negotiated contracts / subcontracts not in excess of TINA ($2.5 Million)
  - With small businesses
  - Price set by law or regulation
  - EPA / NATO, foreign government, etc. contracts
- Must Apply CAS to:
  - Modified CAS – contracts / subcontracts $7.5M to $50M
  - Full CAS – contracts / subcontracts over $50M

CAS in a minute!

- Contracts are subject to CAS – not contractors!



CAS and CMc Contracts for Construction

- CMc = Construction Manager as Constructor Contracting
- GSAR 536.7105-3 Accounting and Auditing Requirements
  - Unless an exemption applies construction contracts under the CMc project delivery method are subject to CAS
  - If CAS does not apply, GSAR 552.236-80, Accounting Records and Progress Payments, will be followed and CAS does not apply.
  - GMP Option Accounting
    - Open book accounting shall be followed for financial tracking of all contract line items that are awarded on a GMP basis.
    - Financial tracking may be accomplished through audit services of the OIG or a CPA

Full vs. Modified CAS coverage – The Difference?

- Current Threshold is $50M
  - Full CAS - Single Award Over $50M
    - All 19 Standards
    - Disclosure Statement
  - Modified CAS
    - 4 basic Standards
    - May need Disclosure Statement
- Full & Modified Require:
  - Consistently cost accounting practices
  - Comply with all CAS
  - Agree to an equitable adjustment for changes to cost accounting practices
  - Agree to an adjustment if not in compliance with the CAS
  - Flow-down to subcontractors

The Disclosure Statement

- Cost Accounting Standards Board (CASB) Disclosure Statement
  - Form DS-1 for commercial organizations
  - Form DS-2 for educational institutions
- When required, the DS provides “disclosure” of chosen CAS-compliant cost accounting practices
- Those cost accounting practices are used to:
  - Measure costs,
  - Accumulate and allocate allowable indirect costs to contracts, and
  - Assign allowable direct costs to contracts
- Requires compliant practice elections and written descriptions

The CAS – Conformance With GAAP

- BASIC Standards
  - CAS 401: Consistency
  - CAS 402: Direct v. Indirect Costs
  - CAS 405: Unallowable Costs
  - CAS 406: Cost Accounting Period
- The Cost Allocation Standards
  - CAS 407: Standard Costs
  - CAS 414: Cost of Money
  - CAS 410: G&A
  - CAS 403: Home Office expenses
  - CAS 418: Direct & Indirect
  - CAS 420: B&P and IR&D
- Asset Accounting Standards
  - ~~CAS 404: Capitalization~~
  - ~~CAS 409: Depreciation~~
  - CAS 417: Self Constructed Assets
- Compensation Standards
  - ~~CAS 408: Compensated Absence~~
  - CAS 412 & 413: Pensions
  - CAS 415: Deferred Comp
- Other Standards
  - ~~CAS 411: Material Costs~~
  - CAS 416: Insurance Costs

CAS Updates / Proposed Changes

- Coverage for IDIQ contracts
- GAAP – Revenue Recognition
- GAAP – Lease Accounting
- Published Agenda:
  - Disconnect from TINA Threshold
  - Consider increase threshold to $25M . . . $50M . . . ???
  - Review 407, 415 and 416 for GAAP Harmonization

Contacts

Douglas Hibshman

Partner, Fox Rothschild
202.461.3113
dhibshman@foxrothschild.com

Bill Walter, CPA

Managing Director |
GovCon Consulting for Forvis Mazars
703.970.0509
bill.walter@us.forvismazars.com

© 2024 Fox Rothschild LLP

Thank you!

Fox Rothschild forvis mazars Marsh

© 2025 Fox Rothschild LLP

Tariffs: Recovering Your Costs and Managing Supply Chain Risk

- Liz Levinson, Partner, Fox Rothschild
- Butch Bracknell, Senior Counsel, Jefferson Lab

© 2025 Fox Rothschild LLP

Which Branch of Government Imposes Tariffs?

- The U.S. Constitution vests Congress with the authority to impose tariffs (often referred to as "duties.")
- Historically, Congress set tariff rates through legislation.
- In the past 70 years, however, Congress has delegated authority to the President, under certain conditions, to adjust tariffs through specific federal statues, including:
    - Section 232 of the Trade Expansion Act of 1962
    - Section 301 of the Trade Act of 1974 (Section 301 tariffs on China from 2020 were just upheld by the Court of Appeals for the Federal Circuit last week in *HTMX Industries v. United States*)
    - The antidumping and countervailing duty statutes (Section 731 and Section 701 of the Tariff Act of 1930)
    - Most recently, President Trump has relied on the International Emergency Economic Powers Act ("IEEPA"). The issue of whether Trump's reliance on IEEPA is constitutional is currently before the U.S. Supreme Court.

Section 232 Duties

- Section 232 of the Trade Expansion Act of 1963 allows the President to impose duties on imported goods that are determined to be a threat to national security (applicable to the entire world!).
- To date, 50% duties have been imposed on steel, and aluminum and copper and "derivative" products thereof (such as nails). Duties of 25% have been imposed on automobile parts. Exceptions for USMCA-specific goods (but those products subject to reciprocal tariffs TBD). On September 29, 2025, President Trump announced new duties of 10% on softwood lumber and 25% tariff on certain upholstered furniture (increasing to 30% on January 1) and on kitchen cabinets and vanities (increasing to 50% on January 1).
- On September 26, 2025, President Trump announced an immediate 100% tariff on branded and patented pharmaceuticals, with an exemption for companies building drug manufacturing facilities in the U.S., as part of a phased approach to encourage domestic production.
- U.S. Court of Appeals for the Federal Circuit affirmed the legality of the Section 232 tariffs on steel imports in *USP Holdings. V. United States*, June 8, 2022. (Supreme Court denied certiorari after Federal Circuit upheld constitutionality).

IEEPA (International Emergency Economic Powers Act)

IEEPA authorizes President to "regulate … importation … of … any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. § 1702(a)(1)(B).

- Must address an unusual and extraordinary threat
- Threat must come from outside the United States
- Threat must be to the national security, foreign policy, or economy of the United
- States
- President must declare a national emergency with respect to such threat"
- IEEPA does not mention "tariffs" as an authorized action
- Constitutionality of Trumps IEEPA tariffs is pending before the U.S. Supreme Court

IEEPA- Eight Major Executive Orders

E.O. 14193 (Feb. 1, 2025) – Northern Border Fentanyl (Canada)
E.O. 14194 (Feb. 1, 2025) – Southern Border Fentanyl (Mexico)
E.O. 14195 (Feb. 1, 2025) – China Fentanyl
E.O. 13829 (Mar. 24, 2025) – Countries Importing Venezuelan Oil
E.O. 14257 (Apr. 2, 2025) – RECIPROCAL TARIFFS—BIG ONE!! AGAINST WHOLE WORLD!
E.O. 14323 (July 30, 2025) – Brazil ("Bolsonaro Tariffs")
E.O. 14329 (Aug. 6, 2025) – India ("Russian Oil Tariffs")
E.O. 14345 (Sept. 4, 2025) – Implementing U.S.-Japan Agreement

IEEPA Litigation

- Court of Appeals for the Federal Circuit held that Trump's reliance on IEEPA to impose tariffs was unconstitutional (*V.O.S. Selections, Inc. v. Trump*, August 29, 2025)
- Constitutional Delegation Issue—Article I, Clause 8 give Congress authority to impose taxes and to regulate commerce with foreign nations.
- President Trump argues that IEEPA gives him the power to "regulate… importation." Federal Circuit held that the power to regulate imports is distinct from the power to impose tariffs
- IEEPA does not expressly authorize the President to imposes tariffs. The statute does not include the words "tariffs" or "duties".
- Fodder for "Strict Constructionists" on the Court, *i.e*. those who stick closely to the literal meaning and original understanding of the founding fathers. (Clarence Thomas, Samuel Alito, Neil Gorsuch and Chief Justice John Roberts)
- Oral Argument Scheduled to November 5, 2025. Possible Decision by end of 2025 or early 2026.

Possible Refunds

- The Trump administration has acknowledged that it will refund all IEEPA tariffs should the Supreme Court find its reliance to be unconstitutional.
- The importers of record paid the tariffs and will be the parties to receive refunds
- Supreme Court is likely to direct Customs and Border Protection ("CBP") to establish procedures for administering the refunds. Huge amount of money at issue. In July 2025, for example, CBP collected over $28.5 billion in duties, representing a 273% increase from last year. Importers who were plaintiffs in the litigation could obtain refunds directly via court order. Non-plaintiffs importers will likely seek refunds through CBP administered procedures.
- Importers of record should keep detailed records about all IEEPA tariffs paid to CBP.
- Importers of record should keep their eyes on "liquidation" dates and file protests where entries are liquidated.
- Refunds will only be applicable to IEEPA duties—not applicable to Section 232 or Section 301 duties

Tariffs = Unplanned Financial Risk to Programs

- Jefferson Lab imports materials, assemblies, and specialized scientific gear routinely from EU states, China, Japan, Canada, and UK
- Tariffs range from 10-30% on products sourced in states from which JLab most often imports
- Additional costs not factored into budget planning
  - Particularly for mid-stream projects in execution.
  - Impacts on project reserve funds removing flexibility to respond to contingencies

Physics Detector Assembly – Imported from Japan

Management of Tariffs

12 GeV accelerator

- Pay the Tariff
  - Causes fiscal pain
  - Cannot allow finance impacts to dictate pace of projects and experiments
- Pay then seek exemptions

o Best exemption: 19 CFR §10.102 and HTSUS 9808.00.50 –

  "Materials Certified to the Commissioner of Customs to be source materials the entry of which is necessary in the interest of the common defense and security."

  - Contracting Officer Self-Certification
  - KO generates certificate USCBP accepts without fail
  - Local, fast, predictable

o Constrained use for Office of Science Labs by DOE Legal Memo

  - DOE memo focuses on "source materials"
  - Term undefined in 19 CFR
  - Imports definition from 40 CFR
  - Does not address the applicability of FAR 52.225-8, which is in JLab's M&O contract

forv/s mazars

Exemptions -- Continued

- Second best exemption: HTSUS 9810.00.60 and 15 CFR 301.8 -- Instruments and apparatus, if no instrument or apparatus of equivalent scientific value for the purposes for which the instrument or apparatus is intended to be used is being manufactured in the United States
- Requires payment of tariff to release import, application post-hoc and request for refund if exemption approved
- Requires application to USCBP via ITA-338P form
- Paper copy, via courier – no electronic submission, no portal
- Extensive documentation to prove up claims in the exemption form – most recent submission was 300 pages
- Long lead times – advised approval timeline is 4-12+ months. Publication in Fed Reg to ensure no domestic sources would have been available
- Application process is a black hole – mailed to an address, no POC, no ability to correspond with a legal reviewer to check status or supplement application

Other mitigation

- Domestic Sourcing
- Preferable regardless of tariffs *if* price and quality are equal to foreign source
  - Easier to reach domestic suppliers for warranty, dispute resolution
  - Shorter supply chain distances, lead times
- BUT policy determination – science should not sacrifice quality to domestic sourcing
  - Seems intuitive
  - Has anyone actually made that decision?

CEBAF (Continuous Electron Beam Accelerator Facility) Upgrade Cryomodule

Contacts

Liz Levinson
Partner

Fox Rothschild
llevinson@foxrothschild.com

Robert Gray Bracknell
Senior Counsel

Jefferson Lab
robertb@jlab.org

© 2024 Fox Rothschild LLP

Thank you!

© 2025 Fox Rothschild LLP

Complying with the Department of Defense's Cybersecurity Maturity Model Certification (CMMC)

October 7, 2025

© 2025 Fox Rothschild LLP

The Panelists

Tom Tollerton, CISSP, CMMC-CA

Principal | IT Risk and Compliance
Forvis Mazars

704.367.7061

tom.tollerton@us.forvismazars.com

Reggie Jones

Partner | Chair of Federal Government Contracts
Fox Rothschild LLP

202.461.3111

rjones@foxrothschild.com

Timothy Marlin

Managing Director | Cyber & Technology E&O
Marsh

917.806.0106

timothy.marlin@marsh.com

© 2024 Fox Rothschild LLP

Alphabet Soup

E.O. 13556 FAR 52.204-21 DFARS 252.204-7021 NIST 800-171 SSP POA&M FCI CUI CTI CDI DOD Instruction 5200.48 NIST 800-172 DOD OUSD(A&S) CMMC UID C3PAO DIBCAC FedRAMP SCC CMMC-AB SPRS

The Goal

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DOD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

89 Fed. Reg. 83092 (October 15, 2024) (Cybersecurity Maturity Model Certification (CMMC) Program)

The Path to Achieve the Goal

- FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)
- DFARS 252.204-7019 (Notice of NIST SP 800-171 DOD Assessment Reqs.)
- DFARS 252.204-7020 (NIST SP 800-171 DOD Assessment Reqs.)
- DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Reqs.)
- DFARS 252.204-7025 (Notice of Cybersecurity Maturity Model Certification Level Reqs.)

What is CMMC?

What is the Cybersecurity Maturity Model Certification (CMMC)?

- A mandatory certification of DOD contractors' and subcontractors' information systems that is intended to protect not only sensitive but also unclassified data against cyber threats.
- Created with federal funding by Carnegie Mellon University & Johns Hopkins University Applied Physics Laboratory, LLC
- CMMC 1.0 released on January 30, 2020
- DOD announced CMMC 2.0 on November 17, 2021
- DOD issued final rule implementing the CMMC program at **32 CFR Part 170** and in the DFARS at 48 CFR Parts 204, 212, 217, and 252
  - Cybersecurity Maturity Model Certification (CMMC) Program (89 Fed. Reg. 83094 (October 15, 2024))
  - Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041) (90 Fed. Reg. 43560 (September 10, 2025))
- Four-phase implementation begins at 48 CFR rule effective date (November 10, 2025)

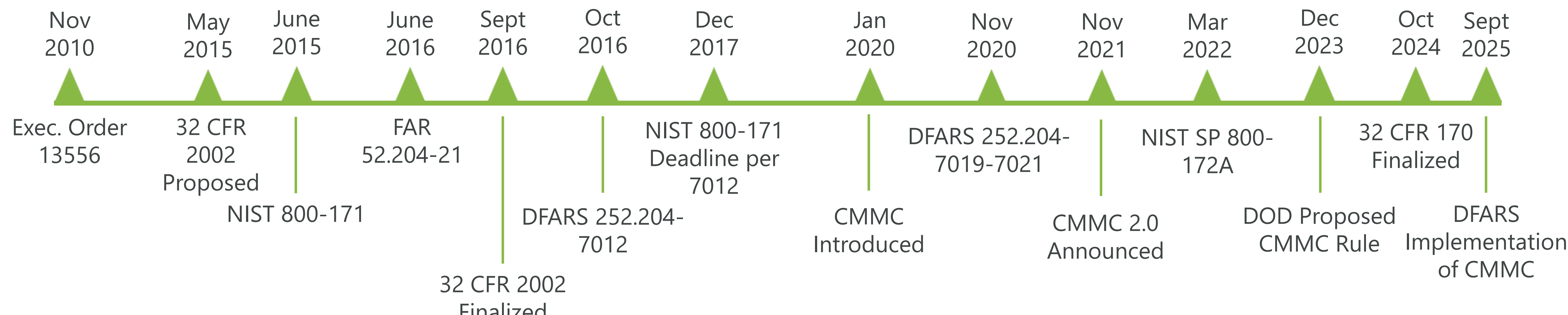
Types of Protected Information

- **Federal Contract Information (FCI)**: "[I]nformation, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments." FAR 4.2901.
- **Controlled Unclassified Information (CUI)**: "[I]nformation the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." 32 CFR 2002.4(h).

CMMC-AB & C3PAOs

- The CMMC Accreditation Body (CMMC-AB) trains and certifies CMMC Third-Party Assessment Organizations (C3PAOs) to assess contractors' processes and practices. Based on those assessments, the CMMC-AB will award Level CMMC certifications. Self-certification is available in some instances.
- C3PAOs will:
  - Explain certification process and provide training
  - Gather information and report metrics on compliance
  - 101 Provisional Assessors were selected by the CMMC-AB to test CMMC certification processes in 2020. https://cmmcab.org/provisional-assessor-lp/
- C3PAO certification is documented in the **Supplier Performance Risk Assessment (SPRS)** at https://www.sprs.csd.disa.mil/

Timeline So Far



- Protecting Controlled Unclassified Information (CUI) has been in process for over a decade.
- The trend is to move from trust (*i.e.*, include in contracts) to verify (*i.e.*, self, then third-party examination by DIBCAC or C3PAOs).
- Implemented at 32 CFR 170 (Cybersecurity Maturity Model Certification (CMMC) Program).
- CMMC entering four-phase implementation rollout beginning November 10, 2025.

Updated CMMC Rollout Timeline

The Final 32 CFR Part 170 and 48 CFR rules have laid out key milestones for the requirement of CMMC compliance.

2024 | 2025 | 2026 | 2027 | 2028

DEC. 16, 2024

32 CFR 170 Rule goes into effect.

C3PAO Assessments Assumed to Begin.

NOV 10, 2025

48 CFR Rule and Phase 1 Begins:
Self-Assessment scores must be submitted to SPRS

C3PAO Assessments optional

NOV 10, 2026

Phase 2:
C3PAO Level 2 Assessments to be required for "applicable DoD solicitations and contracts as a condition of award.

DIBCAC may conduct Level 3 assessments

NOV 10, 2027

Phase 3:
Level 2 Assessments with C3PAO Required for Contractors Given Option Period Extension.

NOV 10, 2028

Phase 4: Full Implementation
All DoD Contracts Will Include CMMC Compliance Requirements.

CMMC Program Levels

CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

Level 1

Contractors handling Federal Contract Information (FCI)

Represents "Foundational" security practices

Level 2

Contractors processing, storing, or handling CUI as part of a DoD contract

Represents "Advanced" security practices

Level 3

Applicable to contractors processing, storing, or handling CUI associated with the most sensitive DoD programs

What Role Does NIST Play?

- The National Institute of Standards & Technology (NIST) is responsible for developing minimum information security standards and guidelines, including for federal systems.
- NIST SP 800-53A (Assessing Security and Privacy Controls for Federal Information Systems and Organizations)(Updated January 2022)
- NIST SP 800-171 Rev. 2 (Protecting Controlled & Unclassified Information in Nonfederal Systems and Organizations) (Updated January 2021)
  - Basic standards
- NIST SP 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information – Supplement to NIST SP 800-171) (February 2021) [First draft issued July 2020]
  - Advanced/expert standards

Practical Tips for CMMC Compliance

- **CMMC Level in Solicitation**: The CO must include in the solicitation the CMMC level that must be met by each contractor information system that processes, stores, or transmits FCI or UCI.
- **CMMC Unique Identifier (UID)**: Each CMMC assessment of contractor information systems entered into SPRS will be assigned a ten-character UID. Contractors must provide with their proposals the UIDs for each information system to be used in the performance of the contract.
- **Affirming Official**: Contractors should maintain an "affirming official" with the authority to affirm the contractor's continuing compliance with the CMMC program.
- **Subcontractor Affirmation of Compliance**: Prior to subcontract award, and annually thereafter, subcontractors must complete an affirmation of compliance with the requisite subcontractor CMMC level. Prime contractors are responsible for subcontractor compliance.
- **Only Store on CMMC-Assessed Systems:** Only store, process, or transmit FCI or CUI in CMMC-assessed information systems of the appropriate level.

Step 1 – CMMC Level Selection

- Once the Program is implemented on November 10, 2025, DOD solicitations will begin to specify the minimum CMMC Status required for eligibility.
- CMMC Statuses:
  - Level 1 (Self) is a self assessment to secure FCI
  - Level 2 (Self) is a self assessment to secure CUI
  - Level 2 (C3PAO) requires the OSA to hire a C3PAO to conduct the assessment to secure CUI (beginning November 10, 2026)
  - Level 3 (DIBCAC) is a government assessment for the security of the most sensitive CUI

Step 2 – Scoping

- Prior to assessment, the CMMC Assessment Scope must be specified in accordance with the requirements of 32 CFR 170.19
- Level 1 Scoping
  - Information systems that process, store, or transmit FCI are in scope and must be assessed.
  - OSA's should consider people, technology, facilities, and External Service Providers within its environment.
- Levels 2 & 3 Scoping
  - Scoping is based on defined asset categories and their respective requirements at Tables 3 to 6 at 32 CFR 170.19.
    - CUI Assets (Levels 2 & 3)
    - Contractor Risk Managed Assets (Level 2)
    - Security Protection Assets (Levels 2 & 3)
    - Specialized Assets (Levels 2 & 3)

Step 3 – Assessment & Affirmation Level 1 (Self)

- Must comply with all 15 requirements of FAR 52.204-21
- Must submit affirmation of compliance into Supplier Performance Risk System (SPRS)
- To maintain CMMC Level 1, the assessment and affirmation must be repeated annually

Step 3 – Assessment and Affirmation Level 2 (Self) & Level 2 (C3PAO)

- Must comply with all 110 NIST SP 800-171 Rev. 2 security requirements
  - Self assessment or assessment by CMMC Third-Party Assessment Organization (C3PAO) depending on scope
- Must submit affirmation of compliance into SPRS annually
- CMMC status will be valid for three years
- Not all requirements need be met immediately
  - If minimum score is achieved (80% of maximum score) and certain critical requirements are met, OSA will receive CMMC Status Conditional Level 2.
  - All unmet requirements must be noted in a Plan of Action and Milestones (POA&M).
  - OSA is eligible for award but must meet all 110 security requirements within 180 days of receiving conditional status.

Step 3 – Assessment and Affirmation Level 3 (DIBCAC)

- Requires both Level 2 and Level 3 assessments
  - Must comply with all 110 NIST SP 800-171 R2 security requirements **AND** 24 selected requirements from NIST SP 800-172
- Assessment conducted by Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)
- Must submit affirmation of compliance into SPRS after each assessment and annually thereafter
- Level 2 and Level 3 assessments must be conducted every three years
- As with level 2, not all requirements need be met immediately
  - Unmet requirements must be addressed in a POA&M and met within 180 days of receiving conditional status

Step 4 – Flow-Down Requirements

- Subcontractors must also have a minimum a CMMC level based on the prime contractor's CMMC level

Prime Contractor Requirements	Minimum subcontractor requirement if the subcontractor will process, store, or transmit:	
	Federal Contract Information (FCI)	Controlled Unclassified Information (CUI)
Level 1 (Self).............................	Level 1 (Self).............................	N/A
Level 2 (Self).............................	Level 1 (Self).............................	Level 2 (Self)
Level 2 (C3PAO).......................	Level 1 (Self).............................	Level 2 (C3PAO)
Level 3 (DIBCAC).....................	Level 1 (Self).............................	Level 2 (C3PAO)

Cyber Security Maturity Model Certification (CMMC) Program, 89 Fed. Reg. 83092 (October 15, 2024)

CMMC Four-Phase Rollout

- Phase 1 begins on November 10, 2025
- Phased approach allows time to train assessors and for contractors to implement CMMC requirements

Phase 1 – Initial Implementation
- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

Phase 2
- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

Phase 3
- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification

Phase 4 – Full Implementation
- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

CIO – About CMMC, https://dodcio.defense.gov/cmmc/About/

Cyber risk environment

Cyber market maturing as insurers analyze loss development and mitigation efforts

- **Market Conditions:** Rates stable; underwriting focused on cyber hygiene and continuous improvements. Coverage scrutiny remains especially around privacy.

- **Market Drivers:** Focus is on catastrophic and third-party risk, dynamic privacy regulations, and continued threat of ransomware.

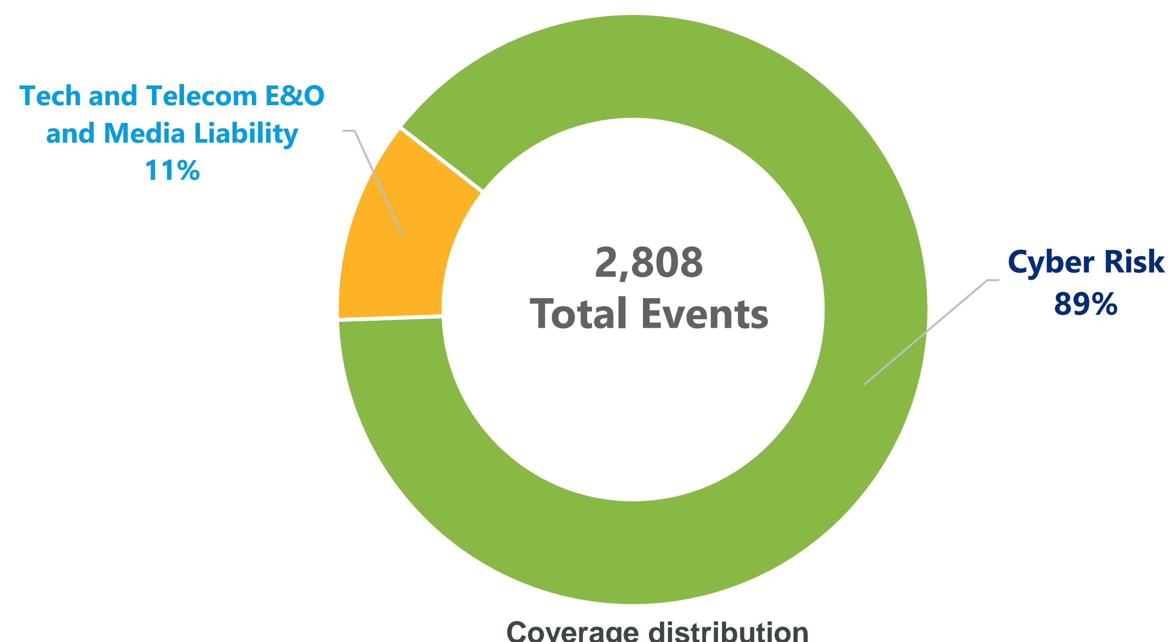
- **Looking Forward:** The cyber market remains strong and mature, even as the risk environment continues to evolve. Reinsurance market in transition as losses continue to increase in frequency and severity. Cyber insurance continues to be an efficient risk transfer solution.

Claims snapshot

Cyber claims and reported events in 2024

2,800+

Cyber events/notifications reported



Coverage distribution

*Analysis based all US and Canada Marsh clients

Trends into 2025

- Growing complexity continues especially related to supply chain events
- Ransomware persists. 11% of notifications reported in 1H ’25 were related to cyber extortion
- Privacy claims are developing and taking longer to settle
- Claims adjustment process related to business interruption is evolving

Claims Snapshot

Cyber claim Ransomware evolutions and reported events in 2024

60%

Percentage of cases that involved lateral movement by threat actors in Q2 2025

74%

Percentage of cases that involved data exfiltration in Q2 2025

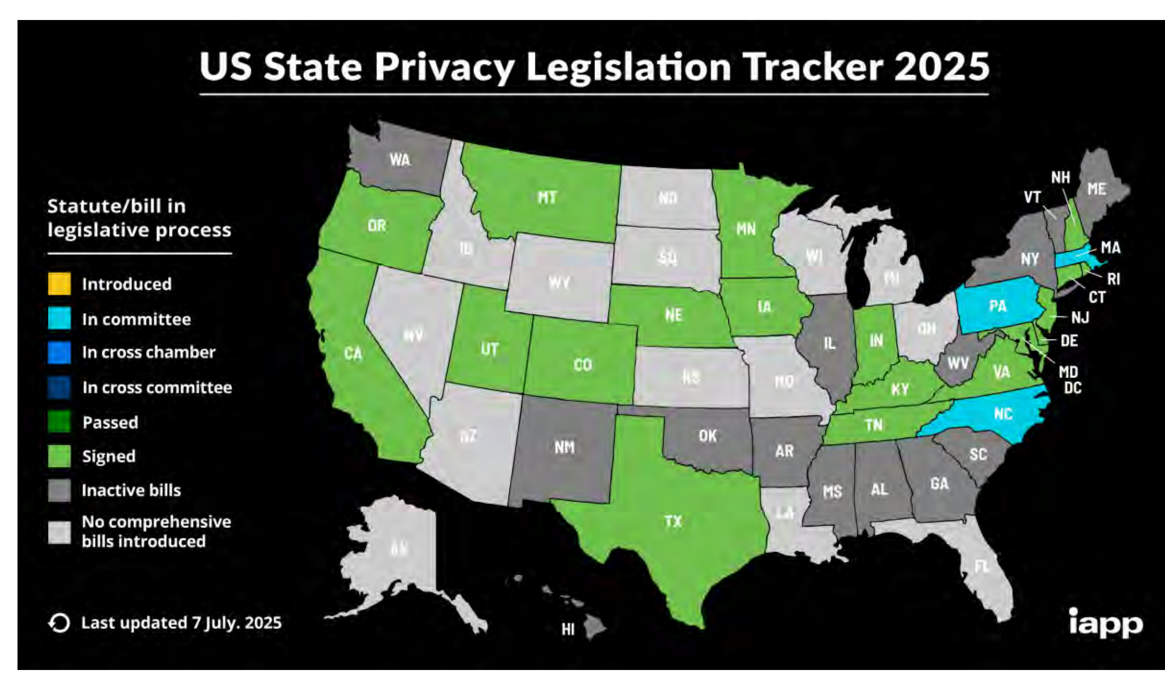
26%

Percentage of ransom payments in Q2 2025

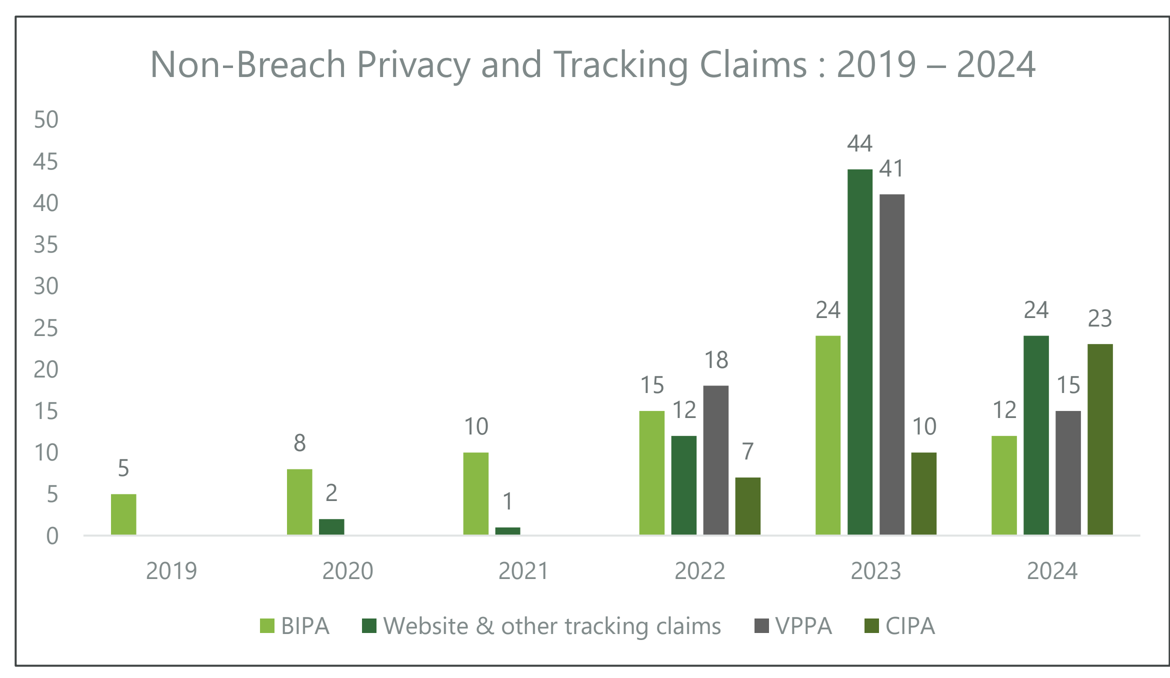
- Source: Coveware

Privacy landscape

Dynamic privacy environment and claims activity are influencing underwriting



In addition to breach notification laws, 19 states have enacted comprehensive privacy laws



Spike in 2023 was driven in part by emerging regulations and new uses of technology. 2024 claims are still developing, and we expect continued flow of privacy related claims in 2025.

- Sources: IAPP; and Marsh US and CAN claims

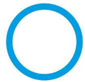
Top cybersecurity controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Evaluate your cybersecurity maturity and prepare for insurance marketing by completing Marsh's Cyber Self-Assessment.
2. Use Marsh Cybersecurity Marketplace Services for access to a curated portfolio of cybersecurity vendor solutions and holistic vendor procurement support.

Multifactor authentication for remote access and admin/privileged controls

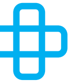


Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

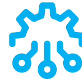


Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

- Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size & industry class.

How Does This All Relate To CMMC? Takeaways?

As the threat environment continues to grow prioritizing efforts will be essential

- The regulatory regime is expanding
- Privacy risk are growing beyond just Personally Identifiable Information (PII) & Confidential Unclassified Information (CUI)
- CMMC is intended to address a key controls for certain exposures exposure, but not every exposure
- Basic hygiene remains essential
- Compliance with CMMC should be used to seek improved terms from the insurance marketplace where possible

What If I Fail to Act?

DOD Memo – June 16, 2022

- *"Contractual Remedies to Ensure Contractor Compliance with DFARS 252.204-7012 for contracts not subject to DFARS 252.204-7020…."*
- *"Failure to have or make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of requirements. Remedies for such breach may include:*
  - *Withholding progress payments;*
  - *Foregoing remaining contract options;*
  - *And potentially terminating the contract in part or in whole."*

Potential Consequences of Noncompliance

- False Claims Act
- Suspension
- Debarment
- CPARS Evaluations
- Soft Consequences
  - Less likely to be awarded a contract if not compliant

False Claims Act Implications

- DOJ is increasing its utilization of the False Claims Act (FCA) to address federal contractors' cybersecurity weaknesses.
- The CMMC provides a uniform set of cybersecurity requirements.
- The CMMC's requirement for a third-party assessment of a contractors' cybersecurity infrastructure provides credible, independent evidence of compliance.

Risks of Noncompliance

- *United States et al v. Morsecorp Inc., et al* (Mar. 2025)
  - $4.6 million settlement for allegedly failing to implement NIST cybersecurity controls, failing to report noncompliance, and using an unvetted company to host emails without ensuring the company met Federal Risk and Authorization Management Program (FedRAMP) requirements.
- *United States ex rel. Doe v. Raytheon Co. et al* (Apr. 2025)
  - $8.4 million settlement to resolve FCA whistleblower suit alleging misrepresentation of cybersecurity compliance deficiencies, including the use of noncompliant internal systems to handle protected information.

Thank you!

© 2025 Fox Rothschild LLP

The Panelists

Tom Tollerton, CISSP, CMMC-CA

Principal | IT Risk and Compliance
Forvis Mazars

704.367.7061

tom.tollerton@us.forvismazars.com

Reggie Jones

Partner | Chair of Federal Government Contracts
Fox Rothschild LLP

202.461.3111

rjones@foxrothschild.com

Timothy Marlin

Managing Director | Cyber & Technology E&O
Marsh

917.806.0106

timothy.marlin@marsh.com

© 2024 Fox Rothschild LLP

Thank you!

© 2025 Fox Rothschild LLP

IEEPA- Eight Major Executive Orders

E.O. 14193 (Feb. 1, 2025) – Northern Border Fentanyl (Canada)
E.O. 14194 (Feb. 1, 2025) – Southern Border Fentanyl (Mexico)
E.O. 14195 (Feb. 1, 2025) – China Fentanyl
E.O. 13829 (Mar. 24, 2025) – Countries Importing Venezuelan Oil
E.O. 14257 (Apr. 2, 2025) – RECIPROCAL TARIFFS—BIG ONE!! AGAINST WHOLE WORLD!
E.O. 14323 (July 30, 2025) – Brazil ("Bolsonaro Tariffs")
E.O. 14329 (Aug. 6, 2025) – India ("Russian Oil Tariffs")
E.O. 14345 (Sept. 4, 2025) – Implementing U.S.-Japan Agreement