Hogan Lovells

Aerospace & Defense Insights

Roadmap for False Claims Act Enforcement in 2024

Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

The Federal Government recovered more than $2.68 billion in Fiscal Year (FY) 2023 from investigations and cases involving the False Claims Act (FCA), a nearly 20% increase over FY 2022. In 2023, the U.S. Department of Justice (DOJ) obtained 543 settlements and judgments — the highest number in a single year and a marked 54.7% increase over FY 2022.

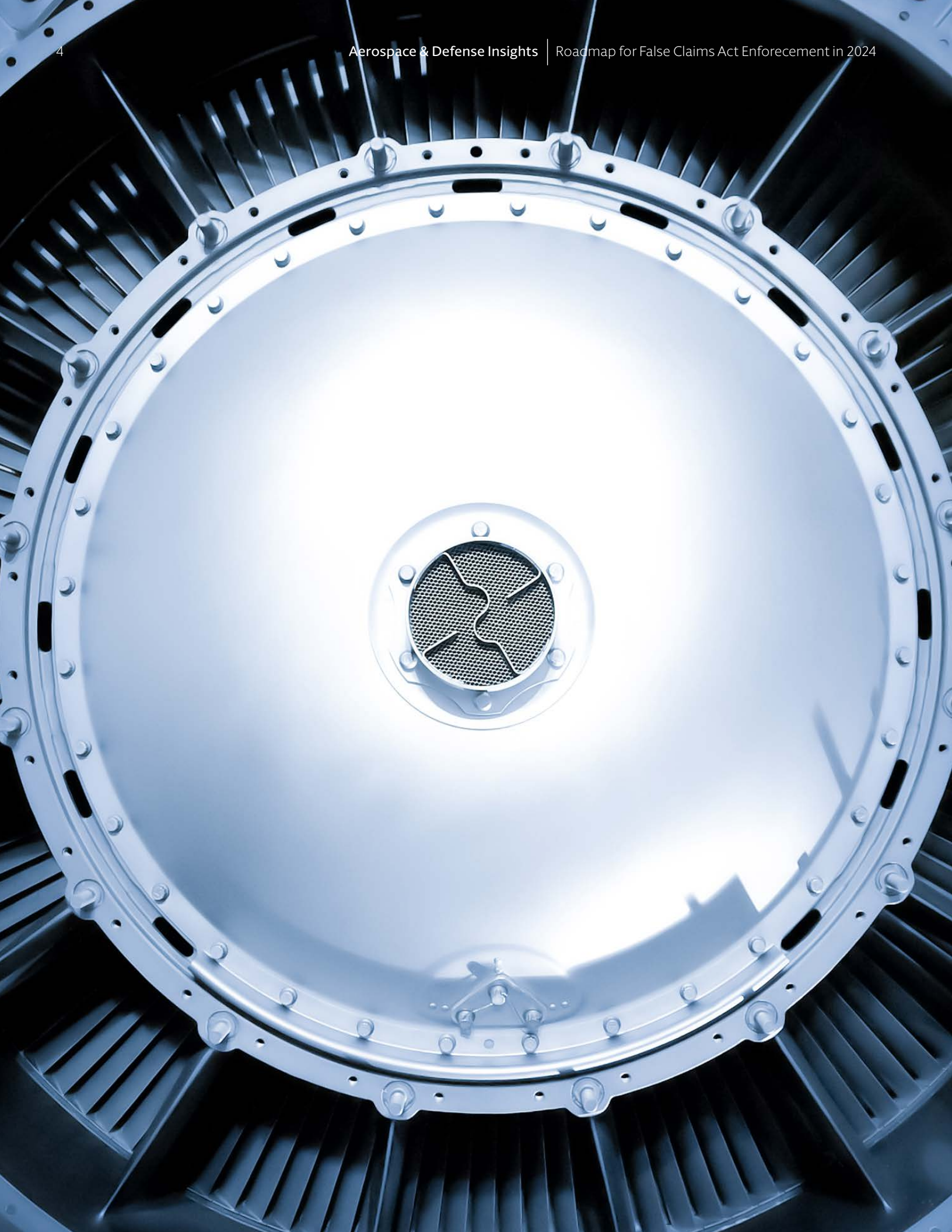
Below, we examine enforcement trends in the A&D industry sector and key FCA-related case law developments that could affect your business.

FCA Enforcement Continues in the A&D Industry

DOJ recovered more than $2.68 billion through settlements and judgments under the FCA in the fiscal year ending September 30, 2023. The government and *qui tam* relators filed 1,212 new cases during FY 2023.[1] Although approximately $1.8 billion of FCA recoveries and enforcement actions were related to healthcare companies, more than $550 million was recovered from A&D companies during FY 2023.

Many of these recoveries reflected DOJ's focus on well-known enforcement priorities, including fraudulent procurement of set-aside contracts, defective products, illegal kickback schemes, and failure to meet cybersecurity requirements under government contracts. Of note, DOJ reached two additional settlements under the Civil Cyber-Fraud Initiative, which is dedicated to utilizing the FCA to combat new and emerging cyber threats.

1 See *U.S. Dep't of Justice, Fraud Statistics Overview* (Feb. 22, 2024),https://www.justice.gov/opa/media/1339306/dl?inline [hereinafter DOJ FY 2023 Statistics].



Federal FCA investigations resolved in FY 2023 that involved A&D companies and other government contractors include the following:[2]

Business	Allegations	Settlement Amount
Management, consulting, and engineering services firm	**Improper charges/overbilling:** Improperly billed commercial and international costs to government contracts.	$377,450,000
Communications equipment manufacturer	**Improper charges/overbilling:** Improperly charged for certain parts twice.	$21,800,000
Architecture and engineering services provider	**Improper charges/overbilling:** Knowingly submitted false claims to the Federal Emergency Management Agency (FEMA) for the replacement of certain educational facilities located in Louisiana that were damaged by Hurricane Katrina.	$11,800,000
Maintenance and operations provider	**Bid-rigging:** Conspired with multiple firms to suppress and eliminate competition by rigging bids and fixing prices for subcontract work under contracts with the U.S. Department of Defense (DoD) by exchanging pricing information and proposal documents.	$8,600,000
Aerospace and aviation company	**Defective services or products**: Falsely claimed compliance with certain contractual manufacturing specifications and requirements related to the procurement of Navy aircraft.	$8,100,000
Research and engineering services provider	**Government set-aside programs**: Knowingly provided false information to the Small Business Administration (SBA) relating to eligibility for federal set-aside contracts intended for small businesses owned and controlled by socially and economically disadvantaged individuals.	$7,700,000
Avionics technology manufacturer	**Overbilling:** Double billed costs under two separate contracts and shifted certain labor and material costs under a series of Navy contacts for the manufacture, design and testing of emerging intelligence, surveillance and reconnaissance technologies.	$4,400,000
Telecommunications provider	**Cybersecurity:** Failed to comply with cybersecurity requirements in connection with information technology services provided to federal agencies.	$4,100,000
Software company	**Kickbacks:** Made improper payments to companies that had a contractual or other relationship with the government that allowed them to influence federal purchases of its own software.	$3,000,000
Medical equipment provider	**Overbilling:** Overcharged the U.S. Department of Veterans Affairs (VA) and DoD for patient monitoring equipment.	$2,500,000
Tactical gear and equipment company	**Domestic preferences:** Failed to comply with requirements of Buy American Act (BAA), Trade Agreements Act (TAA) and Berry Amendment when selling textile-based products to the DoD.	$2,100,000
University	**Failure to disclose foreign interests:** Submitted proposals for federal research grants that failed to disclose current and pending support that multiple faculty members were receiving from foreign sources.	$1,900,000
Graphic design and web services firm	**Cybersecurity:** Failed to secure personal information on a federally funded health insurance website, which the contractor created, hosted, and maintained.	$293,000
Army uniform supplier	**Defective services or products:** Supplied several manufacturers providing DoD with Army Combat Uniforms with permethrin, an insect-repellant, applied to Army uniforms; was required to conduct contractually-required testing to ensure that the level of permethrin it applied to the uniforms fell within the limits specified in the contracts, but instead falsified the records to hide failing tests.	Complaint filed – no settlement reached
	TOTAL	$453,743,000

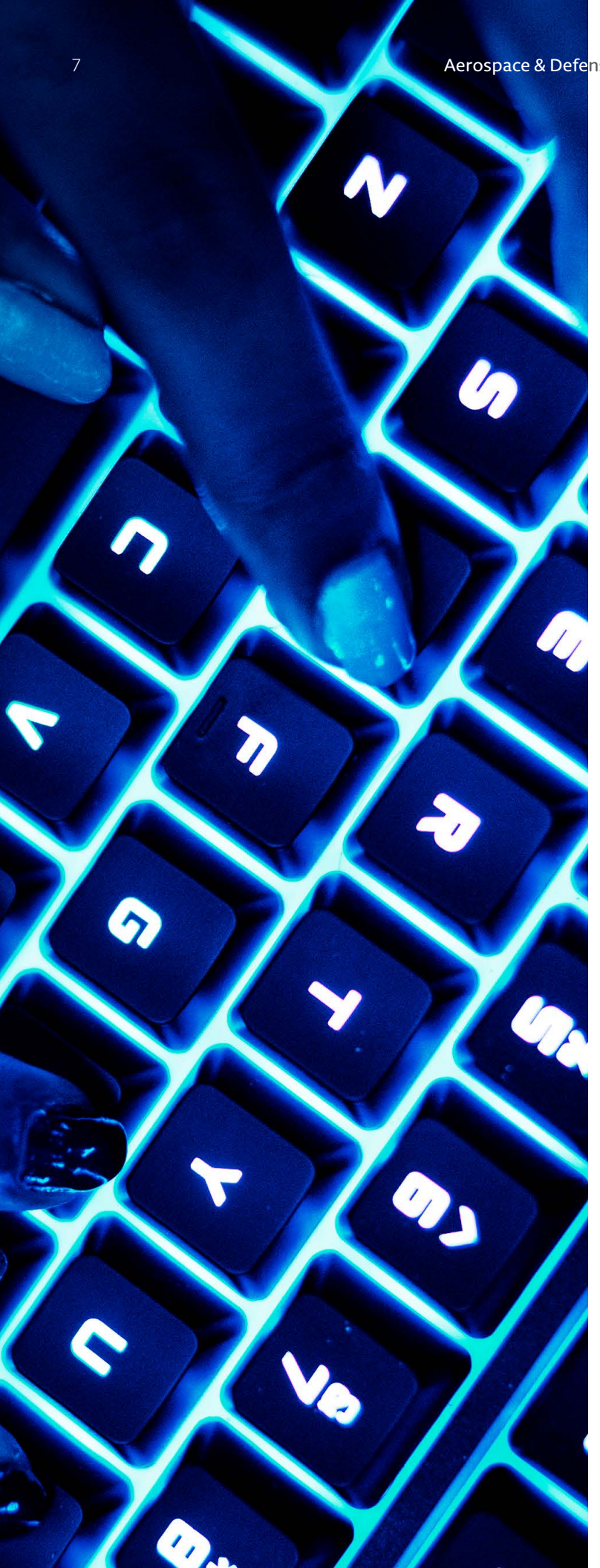
2 *This list captures the most significant and notable settlements in the A&D industry but is not exhaustive. The listed settlement amounts do not include any related criminal fines.*

DOJ Continues to Utilize the FCA to Pursue Cybersecurity Fraud Claims

As we previously wrote in our **2022 Roadmap for False Claims Act Enforcement,** Deputy Attorney General Lisa O. Monaco of DOJ announced the Civil Cyber-Fraud Initiative in October 2021, through which DOJ can utilize the FCA to target cybersecurity-related fraud by government contractors and grant recipients, including by knowingly (1) providing deficient cybersecurity products or services, (2) misrepresenting their cybersecurity practices or protocols, or (3) violating obligations to monitor and report cybersecurity incidents and breaches. DOJ has now brought at least six enforcement actions—including two in 2023—that have led to settlements as part of the Civil Cyber-Fraud Initiative.

DOJ saw its third **settlement** pertaining to the initiative in March 2023 when a Florida-based graphic design and web services provider paid $293,771 to resolve allegations that they failed to secure personal information on a federally funded Florida children's health insurance website for Florida Healthy Kids Corporation (FHKC), which the contractor created, hosted, and maintained. The United States alleged that the contactor not only failed to provide secure hosting of applicants' personal information contrary to its representations in agreements and invoices, but knowingly failed to properly maintain, patch, and update the software systems underlying the website and its related websites between January 2014 and December 2020. The United States also alleged that the contractor was running numerous outdated and vulnerable applications, including some software that had not been updated since 2013. In response to a data breach and the contractor's cybersecurity failures, FHKC shut down the website's application portal in December 2020. As a result of the contractor's failures, more than 500,000 applications submitted on the children's health insurance website were hacked, potentially exposing the applicants' personal identifying information and other data. In September 2023, a telecommunications and internet provider agreed to pay **$4.1 million** to resolve allegations that it violated the FCA by failing to completely satisfy certain cybersecurity controls in connection with information technology services provided to federal agencies under several General Services Administration (GSA) contracts. After learning of the issues, the contractor provided the government with a written self-disclosure and multiple supplemental disclosures, initiated an independent investigation and compliance review of the issues, and cooperated with the government's investigation of the issues and took prompt and substantial remedial measures. The United States acknowledged the cooperation of the contractor, which contributed to the settlement.

In addition to these settlements, universities also faced increased scrutiny under the Civil Cyber-Fraud Initiative. First, on September 1, 2023, the U.S. District Court for the Eastern District of Pennsylvania unsealed a *qui tam* FCA lawsuit (originally filed on October 5, 2022) alleging a state university failed to provide "adequate security" for Covered Defense Information, as required by Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. Although DOJ declined to intervene, this case follows the trend of increased scrutiny surrounding cybersecurity compliance. Second, DOJ recently intervened in its first cybersecurity FCA *qui tam* case, stemming from a July 2022 FCA suit against the Georgia Tech Research Corporation (GTRC) and the Georgia Institute of Technology (GA Tech) by two relators, alleging that the defendants violated the cybersecurity requirements set forth in DFARS 252.204-7012, including failing to implement the 110 required security measures set forth in NIST SP 800-171. Additionally, the relators claim that those in charge of determining if a lab's practices were compliant with NIST SP 800-171 were not only pressured to interpret the controls in a manner that would allow a finding of compliance, but were not qualified to assess or report on compliance, therefore could not produce accurate reports to the DoD. Among other shortcomings, the relators claim that GRC failed to ensure continuous monitoring of compliance during the entirety of contract performance. Following a multiple-year investigation, DOJ intervened in the case in February 2024 leading to the original complaint being unsealed. On August 22, 2024, DOJ filed its own **complaint-in-intervention**, asserting claims that GA Tech and GTRC knowingly failed to meet cybersecurity requirements in connection with DoD contracts.



Avenues for Enforcement Against Government Contractors and Grantees

As demonstrated by the most recent settlements, government contractors and grantees are subject to increased scrutiny of their compliance with cybersecurity requirements, as well as enforcement actions based on alleged failures to meet those obligations. These settlements further underscore concerns that what may have been viewed as breach of contract actions in the past have now shifted into the FCA realm because of the cybersecurity certifications required in government contracts.

Government contractors and grantees may already find themselves subject to cybersecurity requirements requiring substantial investments in data security infrastructure that meets specific standards, including the Federal Acquisition Regulation's (FAR) basic safeguarding clause at 52.204-21 and DoD's safeguarding and cyber incident reporting requirements in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012. Other agencies have recently implemented their own unique cybersecurity requirements for contractors. The Department of Homeland Security (DHS), for instance, implemented a new Homeland Security Acquisition Regulation (HSAR) clause 3052.204-72, *Safeguarding of Controlled Unclassified Information* (Jul 2023), which requires contractors and subcontractors to provide adequate security to protect CUI from unauthorized access and disclosure and to report all known or suspected incidents within one hour if the incident involves personally identifiable information (PII) and eight hours for all other incidents. 88 Fed. Reg. 40,560 (June 21, 2023).

The VA implemented a new clause, VA Acquisition Regulation (VAAR) 852.204-71, *Information and Information Systems Security* (Feb 2023), requiring contractors and others with access to VA information, information systems, or information technology (IT), or providing and accessing IT-related goods and services, to adhere to VA Directive 6500, VA Cybersecurity Program, as well as those set forth in the contract specifications, statement of work, or

performance work statement. 88 Fed. Reg. 4,739 (Jan. 25, 2023). Like the DHS clause, the VA clause also imposes a one-hour notification requirement, in this case for an incident that (i) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or (ii) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. As agencies continue to implement either overlapping or conflicting cybersecurity requirements, the compliance burdens increase and the risk of running afoul of such requirements can also increase, making these areas ripe for scrutiny by the Federal government and whistleblowers.

As we have previously written on **October 13** and **October 26**, 2023, two amendments to the FAR were proposed in October 2023 aimed at implementing portions of President Biden's May 2021 Executive Order (EO) No. 14,028, Improving the Nation's Cybersecurity. The first rule would standardize cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems (FIS). Recognizing the importance of securing FIS – whether cloud based, on-premises, or a hybrid of the two – the proposed rule sets out in great detail cybersecurity policies, procedures, and requirements applicable to contractors that develop, implement, operate, or maintain a FIS. The second rule would require government contractors across all Federal agencies to share information about cyber threats, report cyber incidents, and make representations that they have submitted all security incident reports in a current, accurate, and complete manner. Consistent with the government's focus on scrutinizing cybersecurity noncompliance in terms of fraud, both rules state that compliance with the cybersecurity requirements "is material to eligibility and payment under Government contracts." This broad statement appears to capture the government's position that every aspect of the proposed rules is "material" for FCA purposes, despite the Supreme Court's decision in *Universal Health Services, Inc. v. ex rel. Escobar*, 579 U.S. 176, 191 (2016), confirming that the FCA is not a "vehicle for punishing garden-variety breaches of contract or regulatory violations."

Lastly, DoD released its proposed rule in December of 2023 for updating the **Cybersecurity Maturity Model Certification (CMMC)** program. As confirmed by the rule, DoD anticipates the use of self-attestation, third-party certification, and government-led assessments for cybersecurity compliance. When the certification process begins or is renewed, it is possible that third-party certifiers or DoD may uncover inconsistencies between their assessment and a contractor's own assessment of its security controls. Should the validity of a contractor's own assessment later be questioned, it could leave the contractor vulnerable to a whistleblower claim that alleged false or reckless representations made in the self-assessment caused false claims to be made.

The Meaning of "Knowledge" Under the FCA is No Longer Elusive

In recent years, federal courts have been grappling with the scienter element of the FCA, including how to assess scienter when a statutory, contractual, or regulatory obligation could be interpreted in multiple reasonable ways. The FCA imposes civil liability on persons who knowingly submit false claims for payment to the government. 31 U.S.C. § 3729(a)(1)(A) and (B). The statute defines "knowingly" to mean "actual knowledge," "deliberate ignorance of the truth or falsity of the information," or "reckless disregard of the truth or falsity of the information,"[3] and "requires no proof of specific intent to defraud."[4] In cases where the plaintiff (government or relator) argues that the defendant defrauded the government by relying on an interpretation of an ambiguous term of a statute, contract, regulation, or guidance document, courts have struggled to apply the statutory definition of "knowingly" where the defendant pointed to an objectively reasonable alternative interpretation of the term under which its claim or statement would be true.

The Supreme Court granted certiorari to resolve this question after two Seventh Circuit decisions applied the Supreme Court's analysis of the scienter standard governing another statute to FCA cases. In 2007, the Supreme Court held in S*afeco Insurance Co. of America v. Burr* that relying on an "objectively reasonable" interpretation of a statute does not constitute "reckless disregard."[5] Although *Safeco* involved an interpretation of "willful acts" under the Fair Credit Reporting Act and not the FCA, circuit courts have increasingly been applying the Supreme Court's reasoning in *Safeco* to their analyses of the FCA's knowledge requirement.[6]

In two hotly debated cases – *U.S. ex rel. Proctor v. Safeway*[7] and *U.S. ex rel. Schutte v. Supervalu*[8] – the Seventh Circuit applied the Supreme Court's reasoning in *Safeco* to determine whether defendants acted with reckless disregard for the purpose of establishing FCA liability. The Seventh Circuit held that a defendant faced with an ambiguous statute or regulation does not act with reckless disregard if: (1) the statutory interpretation was "objectively reasonable"; and (2) "authoritative guidance" does not caution against it. The *SuperValu* and *Safeway* cases both involved supermarket pharmacies' interpretation of Medicare's and Medicaid's "usual and customary" price requirements. In both cases, the Seventh Circuit held that the pharmacies' interpretations were objectively reasonable and therefore a finding of FCA scienter was precluded. Importantly, a failure to satisfy the standard for reckless disregard precludes liability under the FCA's actual knowledge and deliberate indifference provisions as well, which concern higher degrees of culpability.[9]

The Fourth Circuit continued the trend of applying *Safeco* to the FCA in *Sheldon v. Allergan Sales, LLC,* 49 F. 4th 873 (4th Cir. 2022). In *Sheldon*, the District Court held that the drug manufacturer relied on a reasonable interpretation of an ambiguous provision of the Medicaid Rebate Program statute and, therefore, did not have the requisite knowledge for

3 Id. § 3729(b)(1)(A).

4 Id. § 3729(b)(1)(B).

5 *Safeco Insurance Co. of America v. Burr,* 551 U.S. 47 (2007).

6 See e.g., *United States ex rel. Streck v. Allergan, Inc.,* 746 F. App'x 101, 106 (3d Cir. 2018); *United States ex rel. McGrath v. Microsemi Corp.,* 690 F. App'x 551, 552 (9th Cir. 2017); *United States ex rel. Donegan v. Anesthesia Assocs. of Kan. City, PC,* 833 F.3d 874, 879–80 (8th Cir. 2016); *United States ex rel. Purcell v. MWI Corp.,* 807 F.3d 281, 284 (D.C. Cir. 2015).

7 *United States ex rel. Proctor v. Safeway, Inc.,* 30 F. 4th 649 (7th Cir. 2022), *cert. granted,* 143 S. Ct. 643 (2023).

8 *United States ex rel. Schutte v. Supervalu Inc.,* 9 F. 4th 455 (7th Cir. 2021) *cert. granted sub nom. United States ex rel. Schutte v. SuperValu Inc.,* 143 S. Ct. 644 (2023).

9 *Safeway,* 30 F.4th at 653.

an FCA violation.[10] On rehearing *en banc*, the Fourth Circuit deadlocked, which resulted in the circuit decision being vacated but the district court's decision in favor of the defendants being upheld.[11]

These contentious decisions led several *qui tam* relators to seek further review on petition for certiorari before the Supreme Court.[12] On 13 January 2023, in light of the circuit split and the government's interest in stopping the current trend, the Supreme Court granted certiorari for the Seventh Circuit opinions in *SuperValu* and *Safeway*.

The U.S. Supreme Court issued its decision in *United States ex rel. Schutte v. SuperValu Inc.,* 598 U.S. 739 (2023) on June 1, 2023, finally answering the question of whether a defendant's "objectively reasonable" interpretation of ambiguous statutory language presents a cognizable defense to "knowledge" under the FCA. As we have **previously** discussed, the Court unanimously vacated decisions from the Seventh Circuit, which held that a defendant does not act knowingly within the meaning of FCA if its conduct is consistent with an objectively reasonable interpretation of an ambiguous statute or regulation. In short, the Court held that the FCA's scienter requirement turns on the defendant's subjective knowledge at the time it presents a claim for payment, so a statute or regulation's facial ambiguity does not by itself preclude FCA liability, regardless of whether the defendant can show an objectively reasonable alternative interpretation after the fact. Beyond that, the Court declined to address many of the other issues presented when a government or whistleblower claim turns on such a facially ambiguous regulation.

Supreme Court Offered Clarity on Governmental Dismissal Authority Under the FCA

For nearly two decades, when DOJ invoked its authority under 31 U.S.C. § 3730(c)(2)(A) to move for dismissal of *qui tam* suits over the objections of the relator who filed it, the DOJ's briefs included argument under at least two different standards of review, thanks to an unresolved circuit split.

On December 6, 2022, the Supreme Court heard oral argument in *U.S. ex rel. Jesse Polansky v. Executive Health Resources, Inc.*, which presented two key questions: (1) whether the government must intervene in order to move to dismiss, and (2) what standard applies if the Government has that authority.[13] The petitioner, Polansky, argued that "the government lacks *any* FCA dismissal authority after initially declining to intervene … because the government has every opportunity to 'proceed' at the outset and control an action, but (consistent with centuries of practice) it has no right to displace the relator's 'exclusive' control after taking a pass in the first instance."[14] In response, the *qui tam* defendants argued that "the Government retains the authority to dismiss a case, even if it initially declined to intervene" and that "the FCA imposes no limitations on when the government may exercise its dismissal authority."[15] The government took a similar position, arguing that the FCA does not require the government to intervene before dismissing an action and that the government's decision to dismiss a *qui tam* action is subject to constitutional, but not statutory, constraints.[16]

---

10 *United States ex rel. Sheldon v. Forest,* 499 F. Supp. 3d 184 (D. Md. 2020).

11 *United States ex rel. Sheldon v. Allergan Sales,* LLC, 49 F. 4th 873 (4th Cir. 2022).

12 See *U.S. ex rel. Tracy Schutte v. SuperValu Inc. (*originating from the Seventh Circuit Court of Appeals, petition for certiorari filed April 1, 2022); *U.S. ex rel. Thomas Proctor v. Safeway, Inc.* (also from the Seventh Circuit, petition for certiorari filed August 3, 2022); *Troy Olhausen v. Arriva Medical LLC* (originating from the Eleventh Circuit, petition for certiorari filed October 18, 2022); *and U.S. ex rel. Deborah Sheldon v. Allergan Sales, LLC* (originating from the Fourth Circuit, petition for certiorari filed December 22, 2022).

13 17 F.4th 376 (3d Cir. 2021), cert. granted, 142 S. Ct. 2834 (2022).

14 See Brief of Petitioner at 4, *Polansky v. Executive Health Res., Inc.* (Aug. 26, 2022) (No. 21-1052) (internal citations omitted).

15 *See* Brief of Respondent Executive Health Resources, Inc. at 16, *Polansky v. Executive Health Res., Inc.* (Oct. 17, 2022) (No. 21-1052).

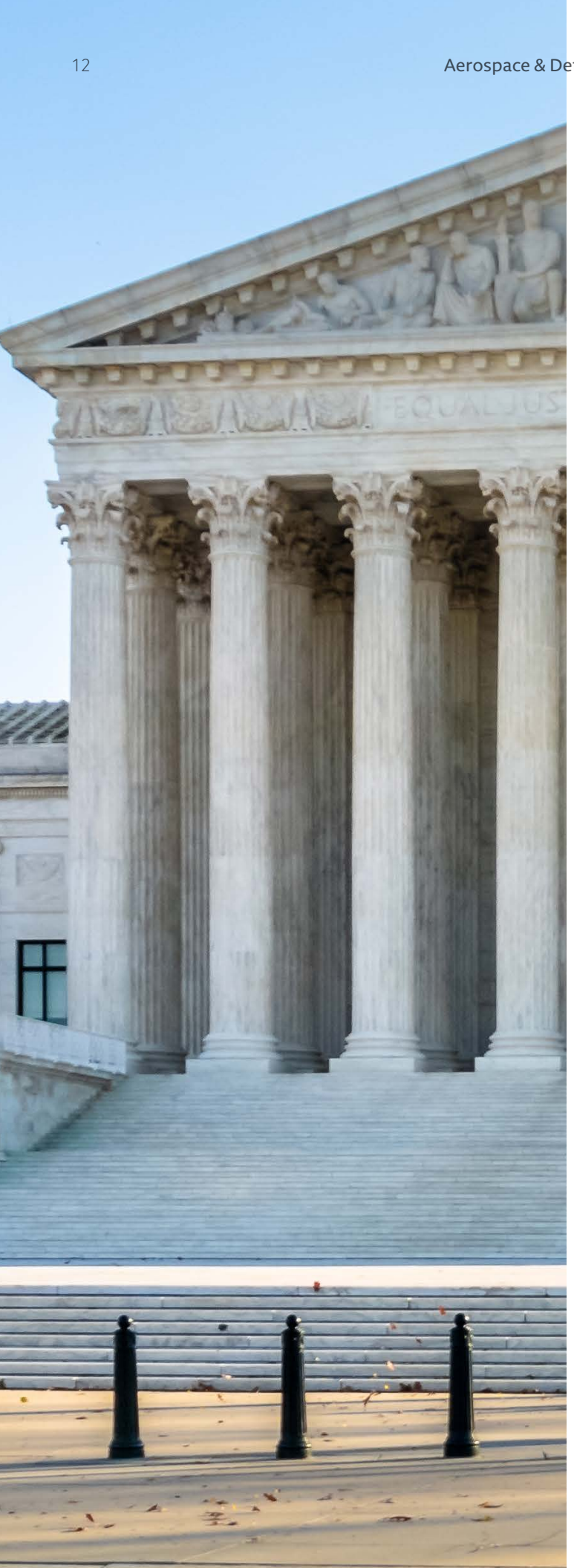
16 See Brief of Respondent United States, Polansky v. *Executive Health Res., Inc.* (Oct. 17, 2022) (No. 21-1052).

As we have **previously** written, the Supreme Court rejected the above-outlined positions in favor of the Third Circuit's "Goldilocks" approach in an 8-1 decision on June 16, 2023.[17] Specifically, the Court rejected the relator's position that the government is barred from filing a motion to dismiss if it initially declines to intervene, explaining that there is no reason to qualify the party status of the government based on whether it intervenes during the initial seal period or later for good cause where the government's interest is always predominant. The Court also rejected the Government's position that it retains "unfettered discretion" to dismiss a *qui tam* complaint at any time. Adopting the Third Circuit's middle path, the Court held that after the government has intervened, it may unilaterally dismiss the *qui tam* lawsuit as long as it meets the relatively modest requirements of Rule 41(a) of the Federal Rules of Civil Procedure. In sum, the Court's decision confirms that the Government has wide latitude to dismiss when it demonstrates that further litigation of a *qui tam* suit is not in the Government's interest. Since the Supreme Court's ruling has set a clear standard for the showing required to dismiss *qui tam* claims, the question now is whether the government will avail itself of the opportunity to exercise the power granted under subsection 3730(c)(2)(A) with any greater frequency than it has historically done.

Next steps

Staying on top of these and other potential developments in FCA enforcement will help inform your organization's compliance, internal investigation, and potential defense posture relating to FCA risk moving forward. Hogan Lovells stands ready to help you with our market-leading lawyers who have deep experience in FCA investigations and litigation and a deep understanding of the Aerospace and Defense industry.

17 See *United States, ex rel. Polansky v. Exec. Health Res., Inc.*, 599 U.S. 419 (2023).



Authors

Stacy Hadeka
Partner
Global Regulatory
Washington, D.C
+1 202 637 3678
stacy.hadeka@hoganlovells.com

Jonathan Diesenhaus
Partner
Litigation, Arbitration, and Employment
Washington, D.C
+1 202 637 5416
jonathan.diesenhaus@hoganlovells.com

Mike Mason
Partner
Global Regulatory
Washington, D.C
+1 202 637 5499
mike.mason@hoganlovells.com

Emily Lyons
Counsel
Litigation, Arbitration, and Employment
Washington, D.C
+1 202 637 6156
emily.lyons@hoganlovells.com

Taylor Hillman
Senior Associate
Global Regulatory
Washington, D.C
+1 202 637 6424
taylor.hillman@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Berlin
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Munich
New York
Northern Virginia
Paris
Philadelphia
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.

*Our associated offices

www.hoganlovells.com