

DoJ's Cyber-Fraud Initiative Targets the Esoteric and Evolving World of Federal Cybersecurity Requirements

By SUSAN B. CASSIDY, ASHDEN FEIN, AARON LEWIS, PETER B. HUTT II, AND RYAN BURNETTE



Susan B. Cassidy



Ashden Fein



Aaron Lewis



Peter B. Hutt II



Ryan Burnette

Introduction

On October 6, 2021, following a series of ransomware and other cyberattacks on government contractors and other public and private entities, the U.S. Department of Justice (DoJ) launched its new Civil Cyber-Fraud Initiative (CFI). As explained by Deputy Attorney General Lisa Monaco and other DoJ officials, the CFI will use the civil False Claims Act (FCA) to pursue government contractors and grantees that fail to comply with mandatory cyber incident reporting requirements and other regulatory or contractual cybersecurity requirements. Monaco emphasized the “hefty penalties” available under the FCA for cybersecurity noncompliance, and stated that “For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it.”¹

Subsequent statements by DoJ lawyers confirm the

continued on page 21

Susan Cassidy, a partner at Covington & Burling LLP, advises on and investigates issues for government contractors at the intersection of government contracts, cybersecurity, and national security. Ashden Fein is a Covington partner who advises on cybersecurity and national security matters. Aaron Lewis is a Covington partner who represents businesses, boards, and individuals in government investigations, internal investigations, and enforcement matters. Peter Hutt is a Covington partner who specializes in False Claims Act defense and cost accounting matters. Ryan Burnette is a Covington special counsel who advises contractors on cybersecurity and other government contract matters.

DOJ'S CYBER-FRAUD INITIATIVE

continued from page 1

broad scope of the CFI. DOJ lawyers responsible for implementing the CFI have publicly stated that their enforcement priorities include the following scenarios:

(1) The government purchases hardware or software with cyber requirements, and the requirements are not met.

(2) A contractor implements IT systems for the government and does not comply with contract requirements, including U.S. citizenship requirements.

(3) A contractor has an IT system that houses government data, and cyber requirements applicable to that system or data are not met.

(4) A contractor is providing cloud services, i.e., through FedRAMP, and requirements are not met.

(5) A contractor fails to comply with regulatory/contractual/statutory requirements to monitor and report cyber incidents and breaches.²

Although these scenarios generally cover the waterfront of potential cybersecurity noncompliance, DOJ leadership has recognized that cyber incidents and breaches may result even when a contractor has a robust monitoring, detection, and reporting system.³ DOJ asserts that the CFI will focus on when contractors or grantees knowingly fail to implement and follow required cybersecurity requirements or misrepresent their compliance with those requirements. With this said, the CFI will likely lead DOJ to take aggressive positions regarding the application of the elements of an FCA violation—i.e., a false claim, materiality, knowledge (*scienter*), and, in certain cases, causation—to alleged noncompliance with cybersecurity requirements. Moreover, DOJ attorneys have publicly stated that they expect that *qui tam* relators will play a “significant role” in CFI by “bring[ing] to light knowing failures and misconduct in the cyber arena” and by providing valuable expertise and insights into the applicable cybersecurity standards and insider knowledge regarding the cybersecurity compliance (or lack thereof) of their employers.⁴ Relators who respond to DOJ’s invitation to bring *qui tam* suits are also likely to assert aggressive positions regarding the FCA’s application to cybersecurity noncompliance.

These *qui tam* suits, coupled with DOJ’s increased emphasis on investigation and litigation of cyber-related FCA cases, will have significant consequences for FCA enforcement in the cyber realm. The cybersecurity requirements applicable to government contractors are complex, esoteric, and constantly evolving, perhaps more so than any other set of requirements applicable to contractors. The proper interpretation and application of these requirements involve not only the judgments and opinions of lawyers, but also the judgments and opinions of IT, cyber, compliance, and other expert professionals. Differences of judgment and opinion will inevitably

arise among these professionals, some of whom may answer DOJ’s call to come forward as relators. FCA cases based on allegations of cyber noncompliance will therefore likely involve differences of opinion and judgment regarding highly complicated technical issues.

As we show below, this will profoundly impact the ability of DOJ and relators to prove the elements of an FCA violation, as well as the ability of defendants to defend against alleged FCA violations.

This article examines the CFI’s likely impact on each element of liability in a cyber FCA case, and also the CFI’s likely impact on the calculation of FCA damages. To set the stage for this analysis, we will start by summarizing the principal cybersecurity requirements currently applicable or likely to become applicable to contractors in the near future.

I. The Landscape of Government Contractor Cybersecurity Requirements

A. Current Requirements

Federal government contractors are currently subject to a variety of cybersecurity safeguarding and reporting requirements. For example, virtually all government contracts from agencies subject to the Federal Acquisition Regulation (FAR), except COTS contracts, now contain the information safeguarding requirements of FAR 52.204-21 (June 2016), “Basic Safeguarding of Covered Contractor Information Systems.” This clause requires contractors to implement 15 basic information security controls derived from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 with respect to covered contractor information systems, which the clause defines as “any information system owned or operated by the contractor that processes, stores, or transmits federal contract information” (FCI). The clause broadly defines FCI to mean information 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, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.” Contractors subject to this FAR Basic Safeguarding Clause are also required to include the substance of the clause in subcontracts under the contract, including subcontracts for commercial items (except COTS items), in which the subcontractor may have FCI residing in or transiting through its information system.

In addition to the FAR Basic Safeguarding requirements, several federal agencies have imposed additional cybersecurity requirements on their contractors through supplements to the FAR or through contract-specific cyber clauses. Some of the most prescriptive of these agency-specific requirements are those imposed in Department of Defense (DoD) contracts (except COTS contracts) by DFARS 252.202-7012 (Dec. 2019), “Safeguarding Covered Defense Information and Cyber

Incident Reporting” (DFARS-7012). This clause first appeared in 2013 and has gone through several iterations. As currently drafted, DFARS-7012 requires DoD contractors to provide “adequate security” for each covered contractor information system, which the clause defines as “an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information” (CDI). The clause further provides that adequate security requires, at a minimum, the contractor to implement the 110 information security controls identified in NIST SP 800-171 (which include the controls that form the basis for the FAR Basic Safeguarding requirements). The clause also requires DoD contractors to “rapidly report” any cyber incident that affects CDI or the contractor information system on which it resides to DoD’s reporting portal within 72 hours of the contractor’s discovery of the

None of these measures has entirely removed the ambiguities and confusion within industry surrounding the precise definitions of CDI and CUI.

incident. DoD contractors subject to the DFARS-7012 clause are further required to include the clause in their subcontracts “or similar contractual instruments” where subcontract performance will involve CDI.

The definition of CDI in the DFARS-7012 clause, which is tied to the various categories of Controlled Unclassified Information (CUI) in the National Archive and Records Administration’s CUI Registry, has caused numerous interpretive and administrative problems for both contractors and DoD.⁵ DoD has attempted to address some of these issues through administrative guidance. One of the most notable examples was the issuance of DoD Instruction 5200.48, which was intended to “establish policy, assign[] responsibilities, and prescribe[] procedures for CUI throughout the DoD.”⁶ However, none of these measures has entirely removed the ambiguities and confusion within industry surrounding the precise definitions of CDI and CUI.

Another interpretive issue that has bedeviled both DoD and contractors is the clause’s requirement that contractors “implement” NIST SP 800-171 “as soon as practical, but not later than December 31, 2017.” Given

the practical difficulties with meeting that deadline as it approached, DoD publicly acknowledged that contractors could demonstrate compliance with this requirement through System Security Plans (SSPs) and Plans of Action and Milestones (POA&Ms) for information systems that included CDI even if they had not fully implemented all 110 security controls for those systems.⁷ However, the degree to which contractors may rely on such POA&Ms (i.e., the number of controls that may be planned for implementation rather than fully implemented) has not yet been tested.

In response to cybersecurity compliance assessments conducted by the Defense Contract Management Agency (DCMA) and increasing cybersecurity threats, DoD imposed additional self-attestations and other cyber requirements on DoD contractors. Effective November 30, 2020, DFARS 252.204-7019 and -7020 require, as a condition of eligibility for award of a DoD contract that will include the DFARS-7012 clause, that offerors must conduct Basic Assessments of their compliance with the 110 NIST SP 800-171 technical controls in accordance with the assessment methodology developed and approved by DoD. These clauses further require such contractors to “score” their compliance according to the numerical scoring system established in the DoD assessment methodology, and to post in the Supplier Performance Risk System (SPRS) the summary scores and certain other information for each contractor information system that will support performance of the contract to be awarded. (Where DCMA has conducted a Medium or High-Level Assessment of the contractor system, DCMA rather than the contractor posts the summary scores for that system.) Contractors are also required to ensure that their subcontractors who will be subject to flowdown of the DFARS-7012 clause post their own summary scores in SPRS (or arrange for the posting of such scores) before any subcontract is awarded.

In addition to requiring Basic Assessments and SPRS score postings, DoD also promulgated DFARS 252.204-7021 in November 2020. This clause was one of the first steps in implementation of DoD’s proposed Cybersecurity Maturity Model Certification (CMMC) program, which would represent yet another evolution of cybersecurity requirements. The requirements of this yet-to-be-implemented program have themselves been evolving. DoD initially released Version 1.0 of the CMMC program on January 31, 2020. Version 1.0 would have required all contractors and their subcontractors (except those selling COTS items) to obtain third-party assessment and certification at one of five maturity levels to be eligible for contracts once the requests for proposals (RFPs) for such contracts contained CMMC requirements. However, DoD subsequently rescinded that version of the program, and in November 2021 announced its new “CMMC 2.0.”

As of publication of this article, this new iteration of CMMC will have three maturity levels (CMMC Levels

1, 2, and 3), with Level 1 corresponding to the security controls required for FCI, Level 2 corresponding to the 110 NIST SP 800-171 security controls required for CDI, and Level 3 corresponding to the 110 NIST SP 800-171 security controls plus some subset of the enhanced security controls required to safeguard against Advanced Persistent Threats by NIST 800-172. Contractors with only FCI on their systems (DoD officials estimate there are approximately 140,000 such contractors) would be required to annually self-attest to the CMMC Level 1 maturity of those systems to be eligible for a contract or subcontract requiring CMMC Level 1 status; contractors with both FCI and CDI on their systems (estimated by DoD to number approximately 80,000 contractors) would either self-attest or be certified by accredited third-party assessors as having CMMC Level 2 maturity on those systems (self-attestations would need to be renewed annually, while third-party certifications would be good for three years); contractors required to meet CMMC Level 3 (estimated by DoD to number approximately 500 contractors) would be assessed and certified by DCMA.⁸ Contractors would not be subject to CMMC requirements until DoD has completed two planned DFARS rulemakings within the next 9–24 months and CMMC requirements are included in the RFPs for particular contracts.⁹ However, DoD has urged contractors with CDI to become “early adopters” of CMMC by voluntarily obtaining third-party CMMC Level 2 certifications before CMMC requirements are imposed in RFPs, and DoD is currently considering various measures that could incentivize contractors to voluntarily adopt CMMC pending completion of the rulemakings. However, even if contractors wanted to obtain third-party certifications early, as of this writing, the program has only certified a very small number of third-party assessors.

B. The Cyber Executive Order

On May 21, 2021, President Biden issued Executive Order (EO) 14028, “Ensuring the Nation’s Cybersecurity” (the Cyber EO).¹⁰ The Cyber EO was issued to address the SolarWinds and other cyberattacks that government agencies and others experienced in late 2020 and the first part of 2021.¹¹ Of particular concern to government contractors, section 2 of the EO requires OMB and other agencies to remove contractual barriers to sharing cyber incident information with the government by updating the FAR language in a manner that requires software providers and IT and operational technology service providers to report cyber incidents and potential cyber incidents to the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) (and possibly other agencies) and to collect, preserve, and share with such agencies information relating to such incidents. The EO also requires DHS and other agencies to review agency-specific cybersecurity requirements and to recommend to the FAR Council standardized contract language for cybersecurity requirements. Finally, section 4

of the EO requires FAR amendments that would prohibit federal agencies from acquiring software, firmware, and products or services containing or using software or firmware that did not meet certain supply chain security best practices, including secure software development practices established by NIST.

The FAR Council has opened two FAR Cases to implement these EO requirements and was originally expected to issue proposed FAR updates in February 2022. That month passed without proposed FAR amendments, but such amendments can reasonably be expected to be proposed in the near future.

In addition to the FAR amendments required by the Cyber EO, the FAR Council has been considering for some time proposing amendments to the FAR that would add to the cybersecurity requirements imposed by the FAR Basic Safeguarding Clause. DoD officials have stated that they expect this rulemaking would impose the 110 NIST SP 800-171 security controls on all government contractors that handle or transmit CUI. Such an amendment would subject all government contractors, and not just DoD contractors, to the NIST SP 800-171 requirements.

C. New Cyber Incident and Ransomware Reporting Legislation

On March 15, 2022, the President signed the Cyber Incident Reporting for Critical Infrastructure Act.¹² The act requires CISA to propose regulations within 24 months after enactment, and to promulgate final regulations within 18 months thereafter, that will require “covered entities” to report “covered cyber incidents” to CISA within 72 hours of the entities’ formation of a “reasonable belief” that the incident has occurred. This rule must also require covered entities to report to CISA any ransomware payment they make as a result of a ransomware attack within 24 hours of the time the payment is made. The act broadly defines the term “covered entity” to include an entity within a critical infrastructure sector as defined in Presidential Policy Directive 21, which includes the Defense Industrial Base, and limits the term “covered cyber incident” to a “substantial cyber incident,” which is one that satisfies the definitions and criteria established by CISA in its final rule. Covered entities are not required to report cyber incidents to CISA if they are required by statute, regulation, or contract to report substantially similar information regarding the incident to another federal agency within a substantially similar timeframe to the 72-hour timeframe established by the act. This exemption will likely lead DOD and other agencies that currently require their contractors to report cyber incidents within 72 hours to leave those requirements in place, and may also leave room for the FAR Council to propose amendments to the FAR adopting across-the-board cyber incident reporting requirements for government contractors pursuant to the Cyber EO while CISA’s rulemaking is pending.

II. What the CFI Likely Means for FCA Enforcement

A. Overview of the False Claims Act

The FCA is the government's principal tool for recovering losses sustained as a result of fraud on the government. The statute imposes liability for treble damages and civil penalties on persons who knowingly submit, or cause to be submitted, a "false or fraudulent" claim for payment.¹³ The statute authorizes the DOJ to bring civil actions in federal district court to recover damages and penalties for violations of the FCA.¹⁴ In addition, the FCA provides for third-party enforcement through "qui tam actions" brought by private parties (called "relators") in the name of the government and entitles relators to share in any damages and penalties that they recover on the government's behalf.¹⁵

Relators are required to file their *qui tam* suits under seal, and the DOJ is obligated to investigate the alleged misconduct.¹⁶ DOJ must then decide whether it will intervene in the case. If DOJ decides to intervene, it becomes the primary party responsible for conducting the litigation, but the relator remains a party and is entitled to share in any damages or penalties recovered. If DOJ decides not to intervene, the relator is responsible for conducting the litigation in the name of the government and is entitled to receive a higher share of any recovery.

The DOJ or relator must prove the following elements by a preponderance of the evidence in order to establish liability for submission of a false or fraudulent claim under the FCA:

1. falsity, i.e., a request for payment (claim) that is false or fraudulent;
2. materiality, i.e., the falsity of the claim must be material to the government's payment of the claim; and
3. scienter, i.e., the false claim must have been submitted "knowingly," which the statute defines to mean that a person has "actual knowledge" of the falsity of the information, acts in "deliberate ignorance" of the truth or falsity of the information, or acts with "reckless disregard" of the truth or falsity of the information.

In addition, in FCA cases alleging that the defendant knowingly submitted false claims by fraudulently inducing the government to award it a contract, courts have required the government to show that the defendant's allegedly fraudulent representation or conduct "caused" the government to award the contract to the defendant ("causation").

There are several ways in which the government or relator can show that a claim is "false or fraudulent." First, a claim can be false or fraudulent if there are factual inaccuracies on the face of the claim regarding the products or services provided ("factually false claim"). Second, a claim that is not factually false can nevertheless be "legally false" if it is based on an express or implied false certification regarding compliance with statutory, regulatory, or contractual requirements. Finally, a claim can be false if it is

submitted under a government contract that was procured by fraudulent misrepresentations or conduct.

In *Universal Health Services, Inc. v. United States ex. Rel. Escobar*, the Supreme Court held that an undisclosed noncompliance with a statutory, regulatory, or contractual requirement can give rise to liability under an "implied certification" if two conditions are met.¹⁷ First, the claim at issue must not merely request payment, but also must make specific representations about the goods or services provided. Second, the defendant's failure to disclose noncompliance with a *material* statutory, regulatory, or contractual requirement makes those specific representations "misleading half-truths." The Court stated that "materiality looks to the effect on the likely or actual behavior of the recipient of the alleged misrepresentation," and identified several factors that it deemed relevant to the determination of materiality, including (1) whether the government had refused payment of the claim or taken other action when it had actual knowledge of defendant's noncompliance or similar noncompliance by other contractors; (2) whether the noncompliance goes to the "essence of the bargain"; (3) whether the noncompliance is a significant one or merely a minor, technical one; and (4) whether the requirement allegedly violated had been expressly designated as a condition of payment.

B. Decisions in FCA Cybersecurity Cases

To date, there have been relatively few FCA decisions involving cybersecurity. Two such decisions are worth examining in some detail because they provide some insight into how courts may apply the FCA to cybersecurity matters: *United States ex rel. Markus v. Aerojet Rocketdyne Holdings*¹⁸ and *United States ex rel. Adams v. Dell Computer Corp.*¹⁹

1. The Aerojet Decision

Brian Markus, a former Aerojet Rocketdyne, Inc. (Aerojet) Director of Cybersecurity, Compliance, and Controls, brought a *qui tam* suit against Aerojet and its parent alleging that Aerojet violated the FCA by misrepresenting its compliance with DoD and NASA cybersecurity requirements. Markus alleged that Aerojet (1) fraudulently induced DoD and NASA into awarding it contracts by misrepresenting its compliance when it entered into those contracts (fraudulent inducement claim) and (2) falsely certified its compliance in requests for payment submitted to DoD and NASA under the contracts (false certification claim). DOJ decided not to intervene in the case, and the court denied Aerojet's motion to dismiss the relator's complaint.²⁰

Aerojet moved for summary judgment on the relator's false certification claim, and both Aerojet and the relator moved for summary judgment on the fraudulent inducement claim and on damages. The court granted summary judgment to Aerojet on the relator's false certification claim because the relator was unable to show that a certification about cybersecurity compliance was made on an

actual claim for payment for any contract under consideration in the case. The court denied summary judgment to either party on the relator's fraudulent inducement claim on the grounds that genuine disputes of material fact existed regarding that claim that precluded summary judgment. The court also denied the parties' motions for summary judgment on damages.

In denying the parties' motions for summary judgment on the relator's fraudulent inducement claim, the court made a number of observations regarding the elements of FCA liability and the parties' contentions that are likely to be cited in future FCA cyber cases. The relator contended that Aerojet's representations regarding its cybersecurity status were false because Aerojet did not disclose the full extent of its noncompliance with the DFARS and NASA cyber clauses. While noting that "the evidence indicates that [Aerojet] disclosed on multiple occasions to the DoD and NASA that it was not compliant with the DFARS clause," the court found the evidence regarding falsity to be contradictory and incomplete in two important respects. First, the court found that evidence concerning a 2013 data breach that affected Aerojet's information systems when it was part of another company created genuine disputes of material fact concerning whether the problems identified in reports on the 2013 breaches were still occurring, whether Aerojet had acted on the reports' recommendations, whether the 2013 breaches had been disclosed to the government, and whether those breaches were relevant to compliance with the applicable regulations. Second, the court found that evidence concerning third-party audits of Aerojet's cybersecurity compliance "does not suggest that [Aerojet] revealed the full picture" of those audits to the government. Accordingly, the court found that a "genuine dispute of material fact exists as to the sufficiency of the disclosures about the 2013 breaches and information gathered in audits"²¹ that precluded summary judgment on the element of falsity.

Regarding the element of materiality, Aerojet argued that materiality was not established merely because the government had expressly incorporated the cybersecurity requirements into the contracts at issue. The court agreed that "the mere fact that a regulation is a [contractual] requirement does not dispositively mean it is a condition of payment or that it is material."²² However, the court stated that "it does not follow that the incorporation of a regulation as a condition of the contract may not be taken into account in determining whether compliance with the regulation is material."²³ The court found that "[h]ere, compliance with the relevant clauses was an express term of the contracts [and] it may be reasonably inferred that compliance was significant to the government because without complete knowledge about compliance, or non-compliance, with the clauses, the government cannot adequately protect its information."²⁴ Accordingly, the court found that a genuine dispute existed as to the materiality element of relator's fraudulent inducement claim.

Regarding scienter, the court found that the relator's evidence "shows that [Aerojet] knew [it] needed to comply with the . . . clauses, and [was] aware of [its] noncompliance and the information obtained through outside audits. Given the evidence cited by relator, and the contradictions in [the] information that [Aerojet] had versus what was presented to the government agencies, [Aerojet] has not demonstrated the absence of a genuine dispute of fact on the scienter element."²⁵

Regarding causation, the court found that "the relator must show actual, but-for causation, meaning defendant's fraud caused the government to contract."²⁶ However, "because of the dispute as to whether [Aerojet] fully disclosed its noncompliance, a reasonable trier of fact could find that the government might not have contracted with [Aerojet], or might have contracted at a different value, had it known what relator argues [Aerojet] should have told the government."²⁷ Consequently, the court denied summary judgment on the element of causation as well.

Finally, regarding damages, the relator contended that he had established damages as a matter of law at over \$19 billion, which was three times the amount of each invoice paid under each contract allegedly obtained by fraud. Conversely, Aerojet contended that there was no evidence that the government suffered any actual damages because the products and services provided under the contracts met the specifications. "In essence, relator would have the court find as a matter of law that what the government received under the contracts had no economic value whatsoever, whereas defendant would have the court find that the government received the full economic value of goods and services [Aerojet] was contracted to provide. The court concluded that "Neither of these propositions is supported by the record before the court." Instead, the court left the quantum of damages for the jury to decide. The case was settled on the second day of trial, with Aerojet agreeing to pay \$9 million plus a confidential amount for attorney fees and an additional confidential amount to settle a separate dispute between Brian Markus and Aerojet.²

2. The Dell Computer Decision

Relator Phillip Adams, a self-described international expert in computer hardware and software systems, brought a *qui tam* action against Dell Computer Corporation.²⁹ The relator argued that Dell violated the FCA by knowingly selling computer systems to the government with system control chips enabling legacy functions that the relator alleged the government did not want or need. According to the relator, these unneeded functions created an undisclosed vulnerability that an attacker could exploit, a vulnerability that the relator described as a "Hardware Trojan."³⁰ The relator asserted that Dell made false statements to induce payment of its claims and false express and implied certifications in connection with its requests for payment. DoJ declined to intervene, and Dell moved to dismiss the complaint.

The court found that the complaint failed to allege any false statements other than the alleged false certifications, and therefore dismissed the relator's false statement theory. The court found that the complaint plausibly alleged a false certification by asserting that Dell's contracts required it to provide defect-free products and that the Hardware Trojan was a defect. However, the court found that the relator had failed to plead facts sufficient to support its allegation of the materiality of this defect. "While it is certainly possible that had the agencies been aware of the Hardware Trojan they would have decided not to purchase the Dell computer systems, an entitlement to refuse the product based on a violation of a contractual requirement is not always material."³¹ Moreover, the court found that "defect-free" was more a policy than a requirement, and that Dell could comply with this policy "by providing a computer system with limited vulnerabilities and providing the necessary assistance to eliminate or reduce vulnerabilities as they appear."³² Therefore, the "existence of a single vulnerability, namely the Hardware Trojan identified by [relator], would not necessarily be material to the agencies' acceptance of the computer systems and payment under the contracts."³³ Furthermore, the relator failed to allege that the government ceased buying computer systems from Dell after the relator disclosed the existence of the Hardware Trojan to DoJ lawyers, and the court found that the continued purchase of computer systems by government agencies even after such disclosures "further supports the Court's finding that [relator] has failed to allege materiality."³⁴

The Dell court also found that the relator's complaint failed adequately to allege the element of knowledge. The court found that relator's allegations that he was "uniquely qualified and singularly able" to identify the Hardware Trojan "directly conflicts with his allegations that Dell knew or should have known that [Dell's] Computer Systems contained the Hardware Trojan."³⁵ Furthermore, the court stated that even if it accepted the relator's conclusion that Dell employees knew that the computer systems contained undocumented programmable functions, the relator had not alleged that those employees had reason to believe the existence of those functions violated a material provision in Dell's agreements with the government agencies. Finally, the court found "implausible" the relator's allegation that Dell deliberately structured its organization to separate individuals with technical knowledge from those involved in negotiating and fulfilling government sales contracts in order to prevent knowledge of technical errors from spilling into the sales force, stating that "Corporate separation of technical and sale [staff] is both common and expected."³⁶

C. Liability and Damages in Cyber FCA Cases

The CFI will likely precipitate more FCA investigations and litigation and will likely increase DoJ's participation in fashioning and pursuing arguments in support of FCA liability and damages in the cyber arena. We now

examine the likely impact of this increased activity on each element of FCA liability and on damages.

1. Impact of CFI on Falsity

The element of falsity will turn on the defendant's compliance or noncompliance with applicable cybersecurity requirements. DoJ or the relator must establish that the defendant failed to comply with particular statutory, regulatory, or contractual cyber requirements as the first step in establishing FCA liability, and defendants can be expected to argue that they in fact complied with the requirements as a clear way to avoid such liability.

Given the complexity and technical nature of the cybersecurity requirements applicable to contractors, the question of whether the contractor complied with those regulations will frequently depend on how those requirements are interpreted. The increased *qui tam* activity resulting from CFI will likely result in assertion of more aggressive interpretations of the cybersecurity requirements than would otherwise have been the case. For example, relators may assert that the DFARS-7012 clause requires contractors to fully implement the NIST SP 800-171 controls by December 31, 2017, while contractors subject to that clause are likely to argue that DoD has acknowledged that the clause requires only that an SSP and POA&M be in place by that date. Relators are similarly likely to assert a broad interpretation of CUI and CDI under the DFARS-7012 clause, while defendants are likely to assert more nuanced interpretations of those terms. DoJ may be compelled to take a position on these and similar interpretive issues. Defendants can work with DoJ and agency lawyers in the process leading up to the intervention decision to persuade DoJ to adopt defendant's interpretive position, or at least to adopt a less aggressive position than that advanced by a relator.

One question that may arise in these discussions is whether the FCA requires "objective falsity." In *United States v. AseraCare, Inc.*,³⁷ the court held that it does, and found "reasonable difference of opinion among physicians reviewing medical documentation [regarding clinical judgments are] not sufficient on [its] own to suggest that those judgments—or any claims based on them—are false under the FCA."³⁸ Therefore, to establish falsity under the FCA in the context of hospital reimbursements, a relator alleging that a patient was falsely certified for hospice care "must identify facts and circumstances surrounding the patient's certification that are inconsistent with the proper exercise of a physician's clinical judgment."³⁹ While other circuits have refused to adopt an "objective falsity" requirement on the grounds that the common law recognizes that an opinion can be considered false for purposes of liability under certain circumstances, these courts acknowledge that the circumstances under which an opinion can be considered false are narrow.⁴⁰ These circumstances include (1) where the opinion is not honestly held; (2) where it implies the existence of facts that do not exist; (3) where it is based on information the physician knew, or had reason to know, was

incorrect; or (4) where no reasonable physician would agree with the opinion based on the evidence.⁴¹

These cases permit a defendant faced with allegations of cybersecurity noncompliance that is based on opinion or judgment to argue that such noncompliance cannot give rise to false claims under the FCA. Contractors may have persuasive arguments that the narrow circumstances under which an opinion or judgment can be false are not present in their case. For example, NIST SP 800-171 controls are often written in a general, nonspecific way. Thus, a contractor may be able to persuasively argue that its opinion or judgment concerning what a particular control requires, or how it should best be implemented, cannot be the basis for falsity under the FCA so long as it was honestly held and other reasonable contractors or professionals would agree with the opinion or judgment based on the facts.

2. Impact of CFI on Materiality

The *Aerojet* decision illustrates the role that CFI is likely to play regarding the materiality element of FCA falsity. Following its announcement of the CFI, the DOJ filed a Statement of Interest (SOI) in *Aerojet* setting forth its views regarding applicability of the *Escobar* materiality factors. The SOI asserted that materiality is not lacking merely because the government continued to pay *Aerojet*'s claims for payment with "some knowledge" of *Aerojet*'s noncompliance because (1) the evidence did not indisputably establish that *Aerojet* disclosed certain details of its noncompliance and that the government was fully aware of the extent of *Aerojet*'s noncompliance when it paid *Aerojet*'s claims and (2) even if the government had been fully aware of the extent of *Aerojet*'s noncompliance, the government allegedly had several good reasons to pay claims and allow the contractor to continue delivering a critical product such as rocket motors. The court accepted these arguments in denying *Aerojet*'s motion for summary judgment on materiality. The court also accepted the SOI's arguments that the government's awareness of cybersecurity compliance problems in the industry and the fact that it modified those requirements several times did not render compliance with those requirements immaterial. Defendants faced with FCA investigations and actions based on alleged noncompliance with these requirements can expect DOJ to advance similar arguments regarding materiality.

In light of the materiality positions taken by DOJ and at least some courts, defendants may want to shift DOJ's and the court's focus to the materiality of compliance with a particular cybersecurity control rather than the extent to which the defendant complied with its cybersecurity requirements as a whole. For example, the NIST SP 800-171 cybersecurity standard referenced in the DFARS-7012 clause has 110 individual controls. These controls do not carry equal weight; DoD has acknowledged as much in assigning them different point values in calculating the compliance assessment scores required to be posted in SPRS under DFARS 7019 and

7020. There should be compelling arguments that failure to comply with a lesser-valued control would not be material to payment. Indeed, DOJ may have difficulty alleging that false scores posted to SPRS are material given the fact that agencies have awarded contracts to offerors with less-than-perfect scores, and the lack of any guidance regarding what score might prove unacceptable.

Proving materiality may be particularly difficult in cases alleging FCA violations for failure to report cyber incidents. Government contractors and subcontractors experience thousands of cyber probes or attacks a week. Determining which of these events to report to DC3 pursuant to the DFARS-7012 clause, for example, requires interpretation of such broad terms as "cyber incident" and "compromise," as well as a technical understanding of the circumstances of each incident, because no two incidents are the same. Even if DOJ or a relator could establish that the contractor had a clear obligation to report a particular incident and failed to do so within the 72 hours from discovery provided by the clause (or at all), they may have difficulty establishing the materiality of that noncompliance under the *Escobar* factors given the lack of apparent effort by agencies to enforce their reporting requirements. In view of this, DOJ and relators may retreat to a position that a failure to report is material where a breach actually occurred and data were exfiltrated, altered, or destroyed.

3. Impact of CFI on Scierter

CFI's greatest impact on the FCA will probably be through its effects on the application of the Supreme Court's decision in *Safeco Insurance Co. of America v. Burr*⁴² to cyber cases. In *Safeco*, the Supreme Court articulated a two-prong test for determining whether a defendant had acted with "reckless disregard" in violation of the Fair Credit Reporting Act. The first prong examines whether the defendant's asserted interpretation of the regulatory obligation in question is "objectively reasonable." If it is, the second prong asks whether authoritative agency or judicial guidance "warned defendant away" from its interpretation. Absent such guidance, a defendant with an objectively reasonable interpretation of the regulation at issue could not be found to have acted with reckless disregard irrespective of its "subjective intent," i.e., its subjective beliefs or understanding regarding the strength of its position.

Several appellate courts have applied the *Safeco* test in determining whether a defendant acted "knowingly" for FCA purposes.⁴³ These courts have not limited the applicability of *Safeco* to determining "reckless disregard" under the FCA; instead, they have treated the *Safeco* test as dispositive of all three subsets of the FCA's knowledge element—actual knowledge, deliberate ignorance, and reckless disregard. Hence, these cases found that once a defendant's interpretation of confusing or ambiguous regulations is found to be objectively reasonable, and there is no formal agency or judicial guidance warning

the defendant away from that interpretation, the defendant cannot have acted “knowingly” for FCA purposes. This is true even where the defendant had not actually based its actions on the interpretation later found to be objectively reasonable.

CFI is likely to affect DOJ’s and the court’s applications of both prongs of the *Safeco* test. The complexity and ambiguity of the cybersecurity regulatory and contractual regimes lend themselves to arguments by defendants that their interpretation of the requirements is objectively reasonable even if legally incorrect. In many cases, the cognizant agencies themselves have acknowledged that their cybersecurity regulations are confusing. DOJ will likely be more receptive than relators to a defendant’s arguments that the regulations are confusing and that a defendant’s interpretation is objectively reasonable. DOJ is likely to leave to relators the burden of challenging the reasonableness of interpretations that actually formed the basis for the defendants’ actions during the relevant period and focus its efforts on those defendants who arrived at their allegedly objectively reasonable interpretations after the fact. This would significantly enhance the prospects of a defendant who followed an objectively reasonable interpretation in avoiding a finding that its false claims were submitted “knowingly.”

By making it more likely that a defendant can show that its interpretation was objectively reasonable, the CFI will put considerable pressure on the second prong of the *Safeco* test, namely whether the agency or a court warned the defendant away from its interpretation. This issue is likely to turn on the source, formality, and clarity of the alleged “warning.” Several courts have insisted that agency guidance must be written and binding on the agency in order to be regarded as sufficient to warn a defendant away from its interpretation.

4. Impact of CFI on Causation

Courts faced with alleged FCA violations based on a fraud in the inducement theory have required DOJ or the relator to show that the alleged fraudulent representations or conduct caused the government to award defendant the contract in question. In *United States ex rel. Cimino v. International Business Machines Corp.*,⁴⁴ the D.C. Circuit held that “but-for” causation is the applicable test for causation in such cases. Under this standard, causation is established by showing that the government would not have entered into the contract (or possibly agreed to the price or terms included in the contract) if it had known of defendant’s allegedly false representations or fraudulent conduct.

DOJ and relators can be expected to argue in fraud in the inducement-type FCA cases that the government is entitled to rely, and in fact does rely, on the express representation of compliance in DFARS 204.7008 and other similar representations in determining whether an offeror is eligible for award of the contract. However, the fact that a government agency may have the discretion

not to award a contract based upon less-than-complete cybersecurity compliance does not mean that the agency would not have awarded the contract had it known of such noncompliance. Instead, whether the agency would have awarded the contract may depend on the particular cybersecurity requirement that is not met, or the degree to which it is not met. In the case of the DFARS clauses, this means the particular NIST SP 800-171 security controls that are or are not fully implemented.

DoD has accepted SSPs and POA&Ms as sufficient demonstrations of compliance even though the defendant may not have fully implemented all of the NIST SP 800-171 controls at the time it submitted its offer. Therefore, it would be difficult for DOJ or a relator to show that the government would not have entered into a contract with an offeror had it known that the offeror had not fully implemented the NIST SP 800-171 requirements. Indeed, there is no evidence that the government has ever refused to award an offeror a contract based on known deficiencies in its compliance with the DFARS-7012 clause. Instead, government agencies appear to have addressed such deficiencies through enhancements to the cybersecurity requirements themselves. Accordingly, it will be difficult for DOJ or relators to prove that the government would not have awarded a contract to a defendant had it known that defendant had failed to fully implement a particular NIST SP 800-171 security control or failed to timely report a particular cyber incident.

5. Impact of CFI on FCA Damages

Increased *qui tam* suits in the cyber area are likely to have important consequences for the calculation of FCA damages and penalties. First, relators have already asserted, and are likely to continue asserting, fraud in the inducement-type FCA claims resulting from allegedly false cyber representations/attestations and other cyber noncompliance. This would allow relators to assert that all requests for payments submitted under contracts induced by the alleged fraud are false claims and that the government’s actual damages equal the full amounts paid as a result of each such false claim. Second, relators may also argue that, in addition to the full amount paid under the fraudulently induced contract, the government’s actual damages include any loss of data or other intellectual property that resulted from any data breach that the defendant allegedly should have prevented and/or reported, plus expenses incurred by the government in responding to, investigating, and remediating the breach.

Defendants can argue that the measure of damages in a fraud in the inducement FCA case is governed by the same principles that govern the calculation of damages in other FCA cases. These principles look to the difference, if any, between the value of what the government was promised versus the value of what it actually received. In the case of a product or service that does not meet applicable specifications, the “diminished value,” if any, is measured by subtracting the value of the product


or service that the defendant actually delivered from the fair market value of the product or service that the defendant would have delivered had it not engaged in the conduct that was found to violate the FCA.⁴⁵ Defendants can argue that, under the *Bornstein* test, the fact-finder cannot disregard the fair market value of the goods or services that the government actually received in determining actual damages, and that only if the value of such goods or services was zero could actual damages be awarded in the full amount paid under the contract.⁴⁶ Defendants can also argue that any other losses suffered by the government, such as from a loss of data or the cost of responding to or remedying a breach, constitute consequential damages that are not recoverable as actual damages under the FCA.⁴⁷

While relators can be expected to assert that cybersecurity noncompliance renders any product or service affected by such noncompliance “worthless,” DOJ is unlikely to assert that proposition as a general matter. Instead, DOJ lawyers responsible for implementing the CFI have publicly stated that damages should be calculated on a case-by-case basis, taking into account the value the government received as well as the value the government did not get as a result of the noncompliance. Only where the product could not be used, as, for example, if the defendant’s knowing cyber noncompliance had allowed an adversarial government to access sensitive data regarding the product, would actual damages equal the full value of the product delivered. In other cases, including failures to report cyber incidents that did not result in the loss of sensitive data, DOJ lawyers have acknowledged that there may be no diminution in value of the product, and that only penalties would be appropriate. They note, however, that where the breach or noncompliance impacted numerous contracts, the amount of the FCA penalties assessed for such breach or noncompliance could be significant.

The “case-by-case” approach to calculating damages is consistent with the SOI filed by DOJ in opposition to defendant’s motion for summary judgment on damages in the *Aerojet* case. In opposing what it described as defendant’s argument that “there can be no damages where [Aerojet] delivered a functional product to the government,” DOJ asserted that this argument “ignores that the government did not just contract for rocket engines, but also contracted with [Aerojet] to store the government’s technical data on a computer system that met certain cybersecurity requirements.”⁴⁸ DOJ asserted that “FCA damages are measured on a case-by-case basis” and are “at least the difference in value between what the government bargained for and what the government received.”⁴⁹ DOJ cited numerous decisions that it characterized as “recogniz[ing] the potential for FCA damages where a defendant has provided a functioning product or required service but failed to satisfy a material requirement.”⁵⁰ DOJ concluded that “if [Aerojet] violated the FCA by failing to provide the cybersecurity required by

the contracts, then the government was damaged because it did not get the full value for which it paid. That is true regardless of whether the government suffered a known loss of data or other cybersecurity breach, even though such a breach could certainly diminish, or conceivably even eliminate, the value of the rocket engines the United States received.”⁵¹

III. Conclusion

Much like federal cybersecurity requirements, theories of liability and potential defenses in cybersecurity-related cases brought under the False Claims Act will inevitably evolve. The highly technical and esoteric nature of proper information system configuration and interpretation of government-mandated controls will undoubtedly make these cases complex both for contractors and for the government. Moreover, the need for contractors to comply with these requirements while simultaneously keeping pace with the constant need to implement new systems and applications increases the chances of a potential noncompliance. Accordingly, contractors should ensure that they not only commit sufficient resources to cybersecurity, but that they do so on a continued basis in order to avoid the specter of FCA liability. 

Endnotes

1. Press Release, Dep’t of Just. Off. of Pub. Affs., Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>.
2. Various Dep’t of Just. speakers, Panel Discussion at Covington (Washington, D.C.), *DOJ’s New Civil Cyber-Fraud Initiative: Government and Relator Perspectives* (sponsored by the Cybersecurity, Privacy, and Data Protection Committee and Procurement Fraud & False Claims Committee of the ABA Public Contract Law Section) (Nov. 9, 2021).
3. Press Release, Dep’t of Just. Off. of Pub. Affs., Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Cybersecurity and Infrastructure Security Agency (CISA) Fourth Annual National Cybersecurity Summit (Oct. 13, 2021), <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>.
4. *Id.*
5. The CUI Registry is accessible at <https://www.archives.gov/cui>.
6. DoD Instruction 5200.48 was issued by the Office of the Under Secretary of Defense for Intelligence and Security on March 6, 2020.
7. Dep’t of Def., Presentation, DoD Industry Information Day, *Protecting DoD’s Unclassified Information—Regulations, Policy and Guidance*, at slide 59 (June 23, 2017) (stating that “[t]he system security plan and any associated plans of action are the mechanism to demonstrate implementation of NIST SP 800-171”), <https://dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940>.
8. Dep’t of Def., *Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward*, 86 Fed. Reg. 64,100 (Nov. 17, 2021).
9. *Id.*
10. Exec. Order No. 14028, *Improving the Nation’s Cybersecurity*, 86 Fed. Reg. 26,633 (May 17, 2021).

11. On December 13, 2020, FireEye announced the discovery of a highly sophisticated cyber intrusion that used a commercial software application made by SolarWinds. Hackers inserted malicious code into an update for SolarWinds' popular network management platform, known as Orion. Customers who routinely updated their Orion software unknowingly downloaded the embedded virus into their systems.

12. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA), Pub. L. No. 117-103, div. Y (Mar. 15, 2022).

13. 31 U.S.C. § 3729.

14. *Id.* § 3730.

15. *Id.*

16. *Id.*

17. 579 U.S. 176 (2016).

18. No. 2:15-CV-02245 WBS AC, 2022 WL 297093 (E.D. Cal. Feb. 1, 2022).

19. 496 F. Supp. 3d 91 (D.D.C. 2020).

20. *United States ex rel. Markus v. Aerojet Rocketdyne Holdings*, 381 F. Supp. 3d 1240 (E.D. Cal. 2019).

21. *Aerojet*, 2022 WL 297093, at *6.

22. *Id.* at *7.

23. *Id.*

24. *Id.*

25. *Id.* at *6.

26. *Id.* at *7.

27. *Id.*

28. Daniel Seiden, *Aerojet Rocketdyne, Whistleblower Settle Cybersecurity Suit (1)*, BLOOMBERG LAW (Apr. 29, 2022, 11:27 AM), <https://news.bloomberglaw.com/federal-contracting/aerojet-rocketdyne-whistleblower-settle-cybersecurity-claims>.

29. Compl., *Adams v. Dell Comput. Corp.*, 496 F. Supp. 3d 91 (D.D.C. 2020) (No. 15-cv-608) (D.D.C. filed Apr. 22, 2015).

30. *See, e.g., id.* at 3.

31. *United States ex rel. Adams v. Dell Comput. Corp.*, 496 F. Supp. 3d 91, 100 (D.D.C. 2020).

32. *Id.*

33. *Id.*

34. *Id.* at 100 n.5.

35. *Id.* at 101.

36. *Id.* at 101 n.6.

37. 938 F.3d 1278 (11th Cir. 2019).

38. *Id.* at 1297.

39. *Id.*

40. *See, e.g., United States v. Care Alts., Inc.*, 952 F.3d 89 (3d Cir. 2020); *United States ex rel. Winter v. Gardens Reg'l Hosp. & Med. Ctr., Inc.*, 953 F.3d 1108 (9th Cir. 2020).

41. *Care Alts.*, 952 F.3d at 97; *Gardens Reg'l Hosp. & Med. Ctr.*, 953 F.3d at 1119.

42. 551 U.S. 47 (2007).

43. *See, e.g., United States ex rel. Sheldon v. Allergan Sales, LLC*, 2022 WL 211172 (4th Cir. Jan. 25, 2022); *United States ex rel. Schutte v. SuperValu, Inc.*, 9 F.4th 455 (7th Cir. 2021); *United States ex rel. Purcell v. MWI Corp.*, 807 F.3d 281, 284 (D.C. Cir. 2015).

44. 3 F.4th 412, 421–22 (D.C. Cir. 2021).

45. *United States v. Bornstein*, 423 U.S. 303, 316 & n.13 (1976).

46. *See, e.g., United States v. Sci. Applications Int'l Corp.*, 626 F.3d 1257, 1269–71 (D.C. Cir. 2010).

47. *Cook Cnty. v. United States ex. rel. Chandler*, 538 U.S. 119, 131 n.9 (2003).

48. *United States' Statement of Interest in Connection with Defendants' Summary Judgment Motion*, No. 2:15-CV-02245 WBS AC, 11 (E.D. Cal. Feb. 1, 2022).

49. *Id.*

50. *Id.* at 20.

51. *Id.*