BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

DOJ's Civil Cyber-Fraud Initiative: The Emerging False Claims Act Landscape For Government Contracting And Cybersecurity

By Alexander O. Canizares and Julia M. Fox[*]

As federal agencies prepare to roll out new regulations to protect government information in the possession of government contractors against cyber threats—and to accelerate the procurement of cybersecurity products and services from industry—the emerging risks of False Claims Act (FCA) investigations and *qui tam* cases related to cybersecurity are an increasingly important consideration for contractors.

The Department of Justice's (DOJ's) Civil Cyber-Fraud Initiative, announced in October 2021, prioritizes enforcement of the FCA against companies and individuals that knowingly violate cybersecurity requirements in government contracts and grants.[1] On March 8, 2022, DOJ announced its first resolution of a cyber fraud case since launching the initiative. Under the settlement, Comprehensive Health Services LLC agreed to pay $930,000 to settle allegations that it violated the FCA by falsely representing to the Department of State and the U.S. Air Force that it complied with contract terms requiring that it maintain a secure electronic system for medical records.[2]

DOJ's focus on cyber fraud comes amid fast-moving changes in the legal landscape related to cybersecurity for government contractors. Russia's ongoing war in Ukraine following its invasion in February 2022 prompted "Shields Up" warnings of the risks of state-sponsored cyberattacks against U.S. companies.[3] On March 15, 2022, President Biden signed into law legislation requiring critical infrastructure owners and operators to report cyber incidents and ransomware payments to the government.[4] The Department of Defense (DoD) is preparing to issue a notice of proposed rulemak-

[*]*Alexander Canizares is a Partner in Perkins Coie LLP's Government Contracts and White Collar and Investigations Practice Groups whose practice focuses on representing government contractors in litigation, investigations, and regulatory compliance involving federal departments and agencies. Julia Fox is an Associate in Perkins Coie's Government Contracts practice group, focusing on government contracts counseling and litigation.*

IN THIS ISSUE:

THOMSON REUTERS®

ing to implement version 2.0 of its Cybersecurity Maturity Model Certification (CMMC) program focused on safeguarding sensitive but unclassified information processed and stored in defense contractors' networks.[5] And the Federal Acquisition Regulatory (FAR) Council is preparing its own rulemaking process to implement President Biden's May 12, 2021 Executive Order on "Improving the Nation's Cybersecurity" (EO 14028)[6] with a view towards adopting standardized cybersecurity contract clauses and cyber incident reporting requirements.

In this shifting environment, the prospect of expanded FCA investigations and litigation related to cybersecurity presents an overlay of compliance risks for government contractors. This BRIEFING PAPER highlights key issues related to DOJ's Civil Cyber-Fraud Initiative within the context of the government's policies to address cyber threats. It also outlines takeaways from recent case law and DOJ policies that will likely be relevant to future cybersecurity fraud cases.

Precedent And Background For DOJ's Civil Cyber-Fraud Initiative

The FCA[7] is a familiar statute for government contractors. Enacted in the 1860s in response to fraud against the Union Army and strengthened by amendments in 1986[8] and 2009,[9] the FCA is the government's primary civil tool to combat fraud against the government. Among other things, the FCA imposes liability on anyone who "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval"[10] or "knowingly makes, uses, or causes to be made or used, a false or fraudulent record or statement material" to a false claim.[11] The statute imposes damages on violators consisting of three times the government's losses plus a statutory penalty for each false claim ranging from $11,803 to $23,607.[12] Each year, DOJ recovers billions of dollars in settlements and judgments under the FCA, with an increasing proportion related to the health care and life sciences industries. In fiscal year 2021 alone, DOJ obtained over $5.6 billion in FCA recoveries, the government's second-largest ever annual total in FCA recoveries.[13]

The government has previously identified priority areas for FCA enforcement. For instance, following the 2008 financial crisis, the DOJ-led Financial Fraud Enforcement Task Force led to years of government investigations, litigation, and settlements with financial institutions under the FCA and the Financial Institutions Reform, Recovery, and Enforcement Act focusing on fraud against federally insured home mortgages and loans.[14] Like that task force, DOJ's Civil Cyber-Fraud Initiative involves a multi-agency coalition focusing on a particular area of fraud, but there are differences. For example, DOJ's cyber initiative will use civil enforcement of the FCA and has the potential to affect contractors and grant recipients in multiple sectors, whereas the financial task force used civil and criminal statutes and was specific to the financial sector.

DOJ's new initiative is not exactly a surprise, as signs of FCA cases involving cybersecurity have emerged in recent years. For example, in a May 2019 decision in *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, the U.S. District Court for the Eastern District of California declined to dismiss a relator's allegations that a defense contractor violated the FCA by misrepresenting its compliance with DoD and National Aeronautics and Space Administration (NASA) cybersecurity

Editor: Valerie L. Gross

Briefing Papers® (ISSN 0007-0025) is published monthly, except January (two issues) and copyrighted by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. Customer Service: (800) 328-4880. Periodical Postage paid at St. Paul, MN. POSTMASTER: Send address changes to Briefing Papers, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

controls in order to fraudulently obtain contracts.[15] As discussed below, the *Markus* case is set to go to trial in April 2022, with important implications for other cybersecurity FCA cases. In late 2020 and early 2021, senior DOJ officials publicly warned that cybersecurity-related fraud was an area of potentially "enhanced False Claims Act activity."[16] The SolarWinds incident[17] and other costly breaches targeting sensitive government data have heightened the sense of urgency to protect sensitive government information against cyber intrusions, and DOJ has embraced the FCA as a key enforcement tool to address the threat.

Against that backdrop, DOJ's Civil Cyber-Fraud Initiative arose out of an ongoing comprehensive cyber review ordered by the Deputy Attorney General (DAG), Lisa O. Monaco, in May 2021.[18] The initiative is being led by DOJ's Civil Fraud Section in the Civil Division's Commercial Litigation Branch, in coordination with other agencies, experts, and law enforcement partners, including agency Offices of Inspector General that investigate waste, fraud, and abuse.[19]

According to DAG Monaco, DOJ's Civil Cyber-Fraud Initiative will use the FCA to hold accountable contractors, individuals, and grant recipients that "put U.S. information or systems at risk."[20] She cited several objectives for the initiative, including building broad resiliency against cybersecurity intrusions, holding contractors and grantees to their commitments to protect government information and infrastructure, and ensuring that companies that "follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage."[21]

A key feature of DOJ's initiative is its reliance on whistleblowers (relators) to identify and bring cases under the FCA's *qui tam* provisions, which allow relators to obtain between 15% and 30% of any settlement or judgment obtained by the government, depending, among other things, on whether DOJ intervenes and takes over the relator's case.[22] DOJ's announcement of the initiative encouraged reports of "tips and complaints" to DOJ.[23] In public remarks on October 20, 2021, DAG Monaco stated: "[T]o those who witness irresponsibility that exposes the government to cyber breaches, our message is this: if you see something, say something. We will use all of the legal authorities in our reach to make you are protected and compensated."[24] The message of encouragement to would-be relators and the relator's bar is unmistakable.

Areas Of Focus For DOJ's Civil Cyber-Fraud Initiative

The Civil Cyber-Fraud Initiative "will focus on cases where federal agencies are victims[,]" according to Brian M. Boynton, then-Acting Assistant Attorney General in DOJ's Civil Division, speaking publicly on October 13, 2021.[25] DOJ has outlined three specific areas of focus.

Deficient Cyber Products Or Services

The first area of focus is the knowing provision of deficient cyber products or services to the government.[26] DOJ has indicated that it will use the FCA to "pursue misrepresentations by companies in connection with the government's acquisition of information technology, software, cloud-based storage and related services" designed to protect the government against cybersecurity threats.[27]

FCA enforcement related to such services and products is particularly noteworthy given the expanding opportunities for commercially available information technology (IT) and cybersecurity solutions sold to federal agencies. Security-focused hardware, software, and services are widely available for sale under the General Services Administration's (GSA) Multiple Award Schedule (MAS) program.[28] More than 10 years into its existence, GSA's Federal Risk and Authorization Management Program (FedRAMP) for cloud security has authorized no fewer than 240 cloud service offerings.[29] President Biden's EO 14028 calls upon agencies to modernize their cybersecurity posture, such as by accelerating their adoption of cloud-based security including for Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS),[30] as well as implementing Zero-Trust architecture and multifactor authentication and encryption.[31]

Vendors seeking to sell commercial cyber products and services in this growing market should be mindful of the heightened FCA risks. As Mr. Boynton explained, government contractors that provide cyber products and services are often required to meet specific contract terms, such as requirements that contractors take measures to protect government data, to restrict non-U.S. citizen em-

ployees from accessing systems, or to avoid using components from certain foreign countries.[32] These comments suggest that alleged failures to comply with Buy American Act or Trade Agreements Act requirements—a frequent area for FCA cases—could become relevant in cyber fraud cases. According to Mr. Boynton, the "knowing failure to meet these cybersecurity standards deprives the government of what it bargained for" and is a "natural fit" for the FCA.[33]

Misrepresentations Of Cybersecurity Practices

The second category of potential liability—knowingly misrepresenting a company's cybersecurity practices or protocols[34]—likewise has broad implications, as illustrated by the pending litigation in *Markus*.[35] As noted above, the relator in that case, a former cybersecurity director with Aerojet Rocketdyne Holdings, Inc. and Aerojet Rocketdyne, Inc., alleges that the defendants fraudulently entered into contracts with DoD and NASA despite knowing that they did not comply with minimum cybersecurity standards set forth in the "Safeguarding Covered Defense Information and Cyber Incident Reporting" clause at Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 in effect as of 2013[36] and in the relevant clause in NASA's acquisition regulations, "Security Requirements for Unclassified Information Technology Resources," at 48 C.F.R. § 1852.204-76.[37] DOJ declined to intervene in the case.[38] But on October 15, 2021, DOJ filed a statement of interest in the case setting forth the government's position on various legal issues in the case implicating the FCA, including materiality and damages.[39]

On February 1, 2022, the district court granted the defendants' motion for summary judgment as to the relator's false certification claim but otherwise declined summary judgment.[40] The case—in which a 15-day trial is scheduled to begin on April 26, 2022—highlights issues likely to arise in other cases.[41] For example, the court allowed the relator to proceed with his promissory fraud theory, according to which liability may attach to each claim submitted to the government under a contract obtained through fraud. The court held that a genuine issue of material fact on this issue existed, stating, "though defendants disclosed noncompliance with the at issue regulations, the extent of the disclosure is unclear from the evidence presented at this stage" and thus summary judgment was not warranted.[42] Promissory fraud is among the likely areas to be litigated in future cybersecurity FCA cases, in part because it has the potential for large damage awards.

Also relevant is the false certification theory of liability based on a defendant's express or implied false certifications of compliance with material contractual, statutory, or regulatory requirements.[43] FCA liability arguably could be triggered, for example, if an entity knowingly misrepresents its cyber compliance in its proposal, or if it submits invoices to the government under its contract knowing—including recklessly disregarding—that it does not comply with certain material cybersecurity requirements set forth in its contract. Contractors that make unsupported or misleading representations to the government regarding the extent of their adoption of standards such as those set forth in National Institute for Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," obviously put them at risk. This is particularly relevant for defense contractors with "covered contractor information systems" that are required under the clause at DFARS 252.204-7020, "NIST SP 800–171 DoD Assessment Requirements," to report to DoD their self-performed scores (Basic Assessments) reflecting the extent of their implementation of the 110 controls set forth in NIST SP 800-171.[44] DoD's newly announced CMMC version 2.0 contemplates self-assessments, third-party assessments, and government-performed assessments to verify contractors' compliance. CMMC will be the subject of a forthcoming rulemaking that could take between 9 and 24 months.[45]

Representations regarding a company's preparedness to address cyber threats appearing in proposals in procurements—and correspondence with the government—also could expose a company to FCA liability, especially to the extent they are relied on by agencies when awarding contracts. As Mr. Boynton noted, companies may make representations to the government "about a system security plan detailing the security controls it has in place, the company's practices for monitoring its systems for breaches, or password and access requirements."[46] According to Mr. Boynton, misreporting of such information may cause the government to "choose a contractor who should not have received the contract" or to "struc-

ture the contact differently than it otherwise would have."[47] He added that knowing misrepresentations "violate the False Claims Act."[48]

Violations Of Cyber Incident Reporting Requirements

The third category of liability—knowingly violating obligations to monitor or report cybersecurity incidents and breaches[49]—implicates the evolving area of disclosure and reporting. Under the "Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019)" clause at DFARS 252.204-7012, defense contractors that possess "covered defense information" (essentially defense CUI)[50] must report cyber incidents to DoD within 72 hours of discovery.[51] Contractors are also required to preserve images of affected information systems when incidents occur.[52] FCA cases theoretically could be premised on allegations that a company—a prime or a subcontractor—knowingly failed to report a cyber incident when required to do so.

There is currently no analogous reporting requirement in the FAR, but that is about to change. As of this writing, the FAR Council is preparing to issue a notice of proposed rulemaking under FAR Case No. 2021-017 to implement sections of President Biden's EO 14028 relating to sharing of information and reporting about cyber threats and incidents.[53] Subject to this forthcoming rulemaking, civilian and defense contractors will likely be subject to new contract clauses focused on notifications of cyber incidents and breaches. In the last year, lawmakers in Congress have proposed several bills intended to strengthen such cyber incident reporting.[54] As noted above, on March 15, 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (Division Y of the Consolidated Appropriations Act, 2022), which requires critical infrastructure owners and operators to report to the Homeland Security's Cybersecurity and Infrastructure Agency (CISA) within 72 hours of any covered "cyber incident" and within 24 hours of making a ransomware payment following a ransomware attack.[55] The law is among the signs that cyber reporting is an area of focus for Congress as well as the Biden Administration.

Key Legal Issues And Considerations

Managing risks associated with government investigations and *qui tam* complaints involving cybersecurity present numerous challenges for companies. Among the key issues to consider are the following.

Attention To Internal Reports Of Misconduct

As *Markus* demonstrates, attention to potential whistleblowers concerning cybersecurity policies and procedures is critical. DOJ's invitation to would-be relators to bring cybersecurity cases highlights the importance of internal controls and effective policies to respond to reports of potential wrongdoing as well as internal disagreements about cybersecurity. As companies are increasingly aware, cybersecurity is not just a matter for the IT department. An effective response to cybersecurity threats increasingly involves multiple corporate functions, including compliance, legal, and management. The universe of possible *qui tam* relators could extend to individuals both inside and outside the company, potentially including partners or competitors.

Exposure For Individuals And Companies

When announcing its Civil Cyber-Fraud Initiative, DOJ specifically noted its intention to hold accountable entities "or individuals" that put U.S. information or systems at risk.[56] It is reasonable to expect that DOJ will bring cases against not only companies but also against employees and others involved in making allegedly false statements related to cybersecurity.

Such an approach is consistent with DOJ policy emphasizing individual accountability for corporate misconduct. During public remarks on October 28, 2021, DAG Monaco confirmed that she had directed DOJ to restore prior guidance explaining that, to be eligible for any cooperation credit, companies "must identify all individuals involved in the misconduct" and not just individuals that are "substantially involved."[57] DOJ has thus reinvigorated the 2015 "Yates Memo" authored by then-DAG Sally Yates, under which DOJ prosecutors and trial attorneys are directed to focus on obtaining individual accountability for corporate wrongdoing.[58] In fact, addressing the American Bar Association's National Institute on White Collar Crime on March 3, 2022, Attorney General (AG) Merrick Garland stressed that DOJ's "first priority in corporate criminal cases is to prosecute the individuals who commit and profit from corporate malfeasance."[59]

Potential liability under the FCA is thus a consideration for company managers and executives involved in signing off on enterprise-wide cybersecurity policies and representations to the government. For example, liability for certain company officials may arise under DoD's version 2.0 of CMMC, subject to the forthcoming notice of proposed rulemaking. Under CMMC 2.0, contractors that do not handle information deemed critical to national security (Level 1 and, possibly, a subset of Level 2) will be required to perform annual self-assessments against certain cybersecurity standards.[60] The results of such a self-assessment must be submitted into DoD's Supplier Performance Risk System on an annual basis with an "affirmation by a senior company official."[61] Inaccurate representations made to DoD could give rise to potential FCA liability.

The FCA does not require specific intent to defraud to establish a violation. Knowledge of a false claim may be proven if a person had actual knowledge, was deliberately ignorant, or recklessly disregarded the falsity of information.[62] Company officials affirming self-assessments and other such statements are well advised to ensure that they are supported by a reasonable inquiry and adequately documented, with the advice of experts and counsel where appropriate.

Sub-Regulatory Guidance, Knowledge, And Materiality

Another emerging issue is the proper role of sub-regulatory guidance to prove an FCA violation. On July 1, 2021, AG Garland issued a memo rescinding a January 2018 policy known as the "Brand Memo," issued by then-Associate Attorney General Rachel Brand, that restricted the use of guidance documents in affirmative civil enforcement cases, a policy he called "overly restrictive."[63] In what is now known as the "Garland Memo," AG Garland made clear that DOJ may not treat agency guidance as having the force of law, but that DOJ attorneys handling enforcement actions and litigation "may rely on relevant guidance documents in any appropriate and lawful circumstances, including when a guidance document may be entitled to deference or otherwise carry persuasive weight" regarding the meaning of a legal requirement.[64]

Guidance documents are relevant to FCA cases for another reason. On January 25, 2022, the U.S. Court of Appeals for the Fourth Circuit (in a 2-1 decision) joined several other circuit courts in holding that "a defendant cannot act 'knowingly' if it bases its actions on an objectively reasonable interpretation of the relevant statute when it has not been warned away from that interpretation by authoritative guidance."[65] Following a 2007 U.S. Supreme Court decision, *Safeco Insurance Co. of America v. Burr*,[66] the Fourth Circuit held that this objective standard "precludes inquiry into a defendant's subjective intent."[67] This issue remains unsettled, however, and further litigation regarding the standard is likely. A related issue that is the subject of recurring litigation among the federal courts is materiality, *i.e.*, the requirement that, for liability to attach under the FCA, the non-compliance must be material to the government's payment decision.[68] How to assess whether and what cybersecurity controls are "material" will be another likely area for legal arguments.

In this context, just what obligations a company has under its contracts related to cybersecurity becomes increasingly important. Non-binding agency guidance documents related to cybersecurity could become a fruitful area for litigation in cybersecurity cases under the FCA. It is reasonable to expect disputes in FCA cases focusing on guidance documents such as NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," and SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information," for non-federal information systems. Key issues may include whether and to what extent a particular standard or control is ambiguous, whether given agency guidance is authoritative, and whether the guidance warned away the defendant from its interpretation. These are among the reasons to monitor new agency guidance related to cybersecurity.

Damages

The proper method for establishing the government's losses is a frequent issue in FCA cases and will likewise be relevant in cases involving government contracting cybersecurity. Although it remains to be seen how courts will ultimately calculate damages arising from suits under DOJ's Civil Cyber-Fraud Initiative, the *Markus* case may provide some insight. At the summary judgment stage in *Markus*, the relator contended that damages total $19 million, amounting to three times the sum of each invoice

paid under each contract obtained through allegedly false statements or fraudulent conduct.[69] In its statement of interest in *Markus*, the government argued that just because a company delivered a functional product to the government does not preclude the government from obtaining FCA damages.[70] As DOJ put it, the "government did not just contract for rocket engines, but also contracted with [the defendant] to store the government's technical data on a computer system that met certain cybersecurity requirements."[71] The defendants contend that there is no evidence that the government suffered any damages. In its decision, the court denied both parties' motions for summary judgment as to damages, finding that damages would be an issue for trial.[72] Whatever the outcome of *Markus*, damages will likely be a relevant issue in future cases.

Final Thoughts

DOJ's Civil Cyber-Fraud Initiative highlights the important role of the FCA in enforcement actions involving the changing legislative and regulatory framework for cybersecurity. Companies can mitigate risks by regularly monitoring their compliance with cybersecurity requirements in their contracts and using gap assessments and other steps to identify shortfalls and overdue implementation of plans of action and milestones. Investing in cybersecurity is the starting point. Implementing effective mechanisms to receive and respond to whistleblower complaints, providing training, documenting decision-making regarding cybersecurity, and preparing for forthcoming regulatory changes are likewise increasingly essential steps.

Guidelines

These *Guidelines* are intended to assist you in understanding compliance risks for government contractors related to DOJ's Civil Cyber-Fraud Initiative. They are not, however, a substitute for professional representation in any specific situation.

1. Regularly review your company's cybersecurity-related contract requirements and develop and, as appropriate, update policies and procedures to ensure compliance with those requirements. Consider communicating with your company's government customer about areas of uncertainty. Consult regulatory guidance and, if necessary, engage outside counsel for assistance.

2. Pay close attention to cybersecurity-related representations in contract terms and conditions, including those required under DFARS 252.204-7012 and -7020, both when preparing to submit a proposal as well as during contract performance.

3. Be attentive to your company's representations concerning its cybersecurity protocols, controls, and practices, including in its Systems Security Plan, and concerning Plans of Action and Milestones (POA&Ms) for implementing measures in the future. If your company is still in the process of developing adequate cybersecurity measures, the government will expect you to be upfront about the status of those efforts. Ongoing monitoring of the status of POA&Ms to ensure their accuracy can reduce the risk of fraud allegations.

4. Conduct regular gap assessments and other steps to identify and remedy cybersecurity shortfalls, while proactively monitoring new developments in cybersecurity. Ensure that company personnel who communicate with government customers are aware of the status of your company's implementation of NIST SP 800-171, as applicable, and other efforts.

5. Ensure adequate controls to receive and respond to whistleblower reports. Provide employees (and others) with adequate channels for reporting, encourage (and express appreciation for) internal reporting, develop a robust anti-retaliation program, and take every report seriously. Information security personnel and those with insight into the company's cybersecurity policies and procedures should be included in these efforts.

6. Educate company personnel on the potential FCA risks associated with cybersecurity non-compliance. Consider including cybersecurity considerations in company training for employees and managers focused on reporting and compliance, including in connection with the company's obligations, as applicable, to disclose credible evidence of violations of the FCA and certain criminal violations under FAR 52.203-13, "Contractor Code of Business Ethics and Conduct."

ENDNOTES:

[1]Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces Civil Cyber-Fraud Initiative (Oct. 6, 2021), https://www.justice.gov/o

pa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (last visited Mar. 6, 2022).

[2]Press Release, U.S. Dep't of Justice, Medical Services Contractor Pays $930,000 To Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan (Mar. 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical (last visited Mar. 15, 2022).

[3]See, e.g., Cybersecurity Infrastructure & Security Agency, Shields Up, https://www.cisa.gov/shields-up (last visited Mar. 13, 2022).

[4]Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y ("Cyber Incident Reporting for Critical Infrastructure Act of 2022"), §§ 101–107, 136 Stat. 49, 1038 (Mar. 15, 2022) (adding subtit. D, "Cyber Incident Reporting," §§ 2240–2246, to Homeland Security Act of 2002, Pub. L. No. 107-296).

[5]U.S. Dep't of Defense, Office of the Under Sec'y of Defense for Acquisition & Sustainment, About CMMC, https://www.acq.osd.mil/cmmc/about-us.html (last visited Mar. 6, 2022).

[6]Exec. Order No. 14028 (May 12, 2021), 86 Fed. Reg. 26633 (May 17, 2021).

[7]31 U.S.C.A. §§ 3729–3733.

[8]False Claims Amendments Act of 1986, Pub. L. No. 99-562, 100 Stat. 3153 (1986) (codified as amended at 31 U.S.C.A. §§ 3729–3733).

[9]Fraud Enforcement and Recovery Act of 2009, Pub. L. No. 111-21, § 4, 123 Stat. 1617, 1621 (2009) (codified as amended at 31 U.S.C.A. §§ 3729–3733); see also Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 10104(j)(2), 124 Stat. 119, 901 (2010) (amending 31 U.S.C.A. § 3130).

[10]31 U.S.C.A. § 3729(a)(1)(A).

[11]31 U.S.C.A. § 3729(a)(1)(B).

[12]Civil Monetary Penalties Inflation Adjustment for 2021, 86 Fed. Reg. 70740, 70742 (Dec. 13, 2021) (adjusting for inflation the penalties under 31 U.S.C.A. § 3729(a)).

[13]Press Release, U.S. Dep't of Justice, Justice Department's False Claims Act Settlements and Judgments Exceed $5.6 Billion in Fiscal Year 2021 (Feb. 1, 2022), https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year (last visited Mar. 6, 2022).

[14]See Exec. Order No. 13519, Establishment of the Financial Fraud Enforcement Task Force (Nov. 17, 2009), 74 Fed. Reg. 60123 (Nov. 19, 2009); see also Press Release, U.S. Dep't of Justice, Justice Department Recovers Nearly $6 Billion From False Claims Act Cases in Fiscal Year 2014 (Nov. 20, 2014), https://www.justice.gov/opa/pr/justice-department-recovers-nearly-6-billion-false-claims-act-cases-fiscal-year-2014 (last visited, Mar. 6, 2022) (noting that DOJ recovered an "unprecedented $3.1 billion from banks and other financial institutions involved in making false claims for federally insured mortgages and loans); see also Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA), Pub. L. No. 101–73, 103 Stat. 183 (1989).

[15]United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019) (Markus I).

[16]U.S. Dep't of Justice, Remarks of Deputy Assistant Attorney General Michael D. Granston at the ABA Civil False Claims Act and Qui Tam Enforcement Institute (Dec. 2, 2020), https://www.justice.gov/opa/speech/remarks-deputy-assistant-attorney-general-michael-d-granston-aba-civil-false-claims-act (last visited Mar. 6, 2022). Mr. Granston explained that when cybersecurity protections are "a material requirement of payment or participation under a government program or contract, the knowing failure to include such protections could give rise to False Claims Act liability." Id.; see also U.S. Dep't of Justice, Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Federal Bar Association Qui Tam Conference (Feb. 17, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-federal-bar (last visited Mar. 15, 2022) ("[C]ybersecurity related fraud may be another area where could see enhanced False Claims Act activity. . . . To the extent that the government pays for systems or services that purport to comply with required cybersecurity standards but fail to do so, it is not difficult to imagine a situation where False Claims Act liability may arise.").

[17]See Cybersecurity Infrastructure & Security Agency, Supply Chain Compromise, https://www.cisa.gov/supply-chain-compromise (last visited April 7, 2022).

[18]Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces 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 (last visited Mar. 6, 2022).

[19]See id.

[20]Id.

[21]Id.

[22]31 U.S.C.A. § 3730.

[23]Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces 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 (last visited Mar. 6, 2022).

[24]U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco and Assistant Attorney General Kenneth A.

Polite Jr. Deliver Opening Remarks at the Criminal Division's Cybersecurity Roundtable on 'The Evolving Cyber Threat Landscape' (Oct. 20, 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr (last visited Mar. 6, 2022).

[25]U.S. Dep't of Justice, 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 (last visited Mar. 6, 2022).

[26]U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces 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 (last visited Mar. 6, 2022).

[27]U.S. Dep't of Justice, Justice Department's False Claims Act Settlements and Judgments Exceed $5.6 Billion in Fiscal Year 2021 (Feb. 1, 2022), https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year (last visited Mar. 13, 2022).

[28]U.S. Gen. Servs. Admin., IT Security, https://www.gsa.gov/technology/technology-products-services/it-security (last visited Mar. 6, 2022).

[29]FedRAMP, FedRAMP Turns 10! (Dec. 8, 2021), https://www.fedramp.gov/blog/2021-12-08/FedRAMP-Turns-10/ (last visited Mar. 13, 2022).

[30]Exec. Order No. 14028, "Improving the Nation's Cybersecurity," § 3 (May 12, 2021), 86 Fed. Reg. 26633, 26635 (May 17, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last visited Mar. 6, 2022).

[31]Exec. Order No. 14028, "Improving the Nation's Cybersecurity," § 3 (May 12, 2021), 86 Fed. Reg. 26633, 26635 (May 17, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (last visited Mar. 6, 2022).

[32]U.S. Dep't of Justice, 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 (last visited Mar. 6, 2022).

[33]Id.

[34]Id.

[35]Markus I, 381 F. Supp. 3d at 1243–44.

[36]The DoD amended DFARS 252.204-7012 in 2015 and subsequently, most recently in 2019, which is the version presently in effect. See "Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019)," DFARS 252.204-7012.

[37]Markus I, 381 F. Supp. 3d at 1244.

[38]Markus I, 381 F. Supp. 3d at 1244.

[39]United States, Statement of Interest, United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., No. 2:15-cv-00245, ECF No. 135 (E.D. Cal. Oct. 20, 2021).

[40]United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., No. 2:15-cv-02245 WBS AC, 2022 WL 297093 (E.D. Cal. Feb. 1, 2022) (Markus II).

[41]Am. Final Pretrial Order, United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., No 2:15-cv-02245, ECF No. 180 (E.D. Cal. Mar. 17, 2022).

[42]Markus II, 2022 WL 297093, at *6.

[43]Universal Health Servs., Inc. v. United States ex rel. Escobar, 136 S. Ct. 1989, 2001–02 (2016).

[44]See DFARS 252.204-7019 (solicitation provision).

[45]U.S. Dep't of Defense, Office of the Under Sec'y of Defense for Acquisition & Sustainment, CMMC FAQs, https://www.acq.osd.mil/cmmc/faq.html (last visited Mar. 15, 2022).

[46]U.S. Dep't of Justice, 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 (last visited Mar. 6, 2022).

[47]Id.

[48]Id.

[49]Id.

[50]See DFARS 252.204-7012(a) (definition of "covered defense information").

[51]DFARS 252.204-7012(c); see DFARS 252.204-7012(a) (defining "rapidly report" as "within 72 hours of discovery of any cyber incident").

[52]DFARS 252.204-7012(c).

[53]Open FAR Cases as of 4/1/2022, at 4, Case No. 2021-017, https://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf (last visited Apr. 5, 2022) (implementing §§ 2(b)–(c), 2(g)(i), and 8(b) of EO 14028).

[54]See, e.g., Cyber Incident Reporting Act of 2021, S.2875, 117th Cong. (2021), https://www.congress.gov/bill/117th-congress/senate-bill/2875/text (last visited Mar. 6, 2022); Cyber Incident Notification Act of 2021, S.2407, 117th Cong. (2021) https://www.congress.gov/bill/117th-congress/senate-bill/2407/text (last visited Mar. 6, 2021).

[55]Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y ("Cyber Incident Reporting for Critical Infrastructure Act of 2022"), § 103, 136 Stat. 49, 1038 (Mar. 15, 2022) (adding § 2242 to Homeland Security

Act of 2002, Pub. L. No. 107-296, to be codified at 6 U.S.C.A. § 681b).

[56]Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces 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 (last visited Mar. 6, 2022) (emphasis added).

[57]U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Gives Keynote Address at ABA's 36th National Institute on White Collar Crime (Oct. 28, 2021), https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute.

[58]See Memorandum from Sally Quillian Yates, U.S. Deputy Att'y Gen., U.S. Dep't of Justice, Individual Accountability for Corporate Wrongdoing (Sept. 9, 2015), https://www.justice.gov/archives/dag/file/769036/download.

[59]See U.S. Dep't of Justice, Remarks as Delivered by Attorney General Merrick B. Garland to the ABA Institute on White Collar Crime (Mar. 3, 2022), available at https://www.justice.gov/opa/speech/attorney-general-merrick-b-garland-delivers-remarks-aba-institute-white-collar-crime.

[60]U.S. Dep't of Defense, Office of the Under Sec'y of Defense for Acquisition & Sustainment, CMMC Assessments, https://www.acq.osd.mil/cmmc/assessments.html (last visited Mar. 14, 2022).

[61]U.S. Dep't of Defense, Office of the Under Sec'y of Defense for Acquisition & Sustainment, CMMC FAQs, https://www.acq.osd.mil/cmmc/faq.html (last visited Mar. 15, 2022).

[62]31 U.S.C.A. § 3729(b)(1).

[63]Memorandum from Merrick Garland, U.S. Att'y Gen., U.S. Dep't of Justice, Issuance and Use of Guidance Documents by the Department of Justice 2 (July 1, 2021), https://www.justice.gov/opa/page/file/1408606/download (last visited Mar. 14, 2022).

[64]Id. at 2–3.

[65]United States ex rel. Sheldon v. Allergan Sales, LLC, 24 F.4th 340, 348 (4th Cir. 2022).

[66]Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47 (2007).

[67]Sheldon, 24 F.4th at 348.

[68]Universal Health Servs., Inc. v. United States ex rel. Escobar, 136 S. Ct. 1989, 2001–02 (2016).

[69]Markus II, 2022 WL 297093, at *8.

[70]United States, Statement of Interest at 11–13, United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., Case No. 2:15-cv-00245, ECF No. 135 (E.D. Cal. Oct. 20, 2021).

[71]Id. at 11.

[72]Markus II, 2022 WL 297093, at *8.

NOTES:

BRIEFING PAPERS