Privacy & Cybersecurity
Alert

Weil

March 15, 2022

# Spotlight on DOJ's Cybersecurity Focus

*By Drew Tulumello, Arianna Scavetti, and Jason Kleinwaks**

In recent years, corporate attention to cybersecurity and data privacy issues has become imperative. Companies are confronting increased regulation and enforcement of data practices worldwide, as well as increased legal and reputational risk from data breaches and resulting litigation. Consistent with these trends, cybersecurity has emerged as a major focus of the Biden Administration. In May 2021, the White House issued an Executive Order entitled "Improving the Nation's Cybersecurity." The Executive Order focused on improving the cybersecurity and data sharing of agencies and contractors. For example, the Executive Order called on NIST to examine cybersecurity labeling criteria for Internet-of-Things devices; the Executive Order also emphasized contractors' responsibilities to "promptly report" the discovery of cyber incidents involving software or software-support provided to an agency. This Executive Order was partially a response to the Solar Winds hack, and followed only days after the disruptive Colonial Pipeline ransomware attack.

In October 2021, the Department of Justice (DOJ) announced the launch of its Civil Cyber-Fraud Initiative, led by the Commercial Litigation Branch of the Fraud Section within the DOJ's Civil Division. DOJ declared its intent to utilize the False Claims Act to combat cybersecurity-related fraud by government contractors and grant recipients. DOJ has previously brought actions against contractors for misrepresentation of their software capabilities. For example, in 2019, IBM agreed to pay nearly $15 million to settle allegations that it misrepresented its software capabilities when bidding for a contract to develop Maryland's health insurance exchange website; also that year, Greenway Health, a Florida-based software developer, agreed to pay $57.25 million to settle claims it had misrepresented the capabilities of its electronic health records product. With the Civil Cyber-Fraud Initiative, DOJ signals a newfound emphasis on cybersecurity specifically.

Against this backdrop, government attorneys shared their views on developments and trends in False Claims Act litigation at the Federal Bar Association's 2022 Virtual Qui Tam Conference. Among the areas of focus was the use of the False Claims Act as a weapon against cybersecurity fraud. Colleen Kennedy, Deputy Chief in the Civil Division at the U.S. Attorney's Office for the Eastern District of California (Sacramento) and a member of a cross-agency cybersecurity working group, and other private practitioners in the space shared some insight into the government's approach to cybersecurity and potential fraud. Slides from their discussion are attached here.

** Associate Nathan Bu assisted with drafting this article*

The following are some key takeaways to mitigate risk and avoid straying into the government's crosshairs:

- **All government contractors must be particularly attentive to cybersecurity issues:** With the Civil Cyber-Fraud Initiative, cybersecurity is now an "enforcement priority." While "the Initiative is not imposing anything new on industry" in terms of expectations or requirements, the government is dedicating substantial resources to cases in this area. Importantly, the Initiative is not limited to investigating contractors that provide cybersecurity products or services. The Initiative will also take action against contractors that either "knowingly misrepresent their cybersecurity practices" or "knowingly violate their obligations to monitor and report cybersecurity incidents."
- **Contractors must carefully review information they provide to the government about their cybersecurity capacity:** The government's focus on cybersecurity goes beyond the mere occurrence of a cybersecurity breach. Independent of whether a breach occurred, the government is also laser-focused on whether a contractor knowingly failed to comply with the government's cybersecurity requirements or knowingly misrepresented its security controls. This was the case in *United States ex rel. Markus v. Aerojet Rocketdyne, Inc.*, 2:15-cv-2245 WBS-AC (E.D. Cal.), which is set for trial in April 2022. In that case, the contractor allegedly failed to disclose its inability to meet the government's cybersecurity requirements when seeking government contracts, potentially giving rise to False Claims Act liability. As many agencies require an affirmative statement or certification, such as a **Cybersecurity Maturity Model Certification**, contractors are reminded to carefully evaluate any affirmative statements or certifications made in securing a contract to ensure accuracy.
- **Prompt disclosure of any cybersecurity breaches are essential:** When breaches or other issues do arise, the government encourages contractors "to self-report and to come forward to deter bad actors from taking advantage of vulnerabilities that may exist." Whether a breach was concealed or ignored will also be a critical factor for the government in deciding whether to pursue a False Claims Act case against a contractor. Although contract- and agency-dependent, breaches typically should be reported within 72 hours of discovery. Many contracts with the Department of Defense also require contractors to facilitate a damage assessment after a breach, in order to determine what information may have been affected by a breach and to monitor emerging cyber-threats.
- **While specific cybersecurity requirements will be contract- and agency-dependent, the NIST Cybersecurity Framework remains the gold standard:** The National Institute of Standards and Technology's Cybersecurity Framework, NIST 800-171, predominates in federal contracts, especially those with the Department of Defense. Contractors are encouraged to familiarize themselves with the NIST Cybersecurity Framework; however, each contract with the government should be carefully reviewed to ensure the applicable standards are clear at the outset.

Ongoing monitoring and auditing of cybersecurity practices will be particularly critical to mitigating risk. Weil has broad capabilities to help implement and audit cybersecurity practices, investigate potential lapses or breaches, and defend against related litigation. If you have questions concerning the contents of this alert or would like more information about Weil's Complex Commercial Litigation, Privacy & Cybersecurity, or White Collar Defense, Regulatory, and Investigations practice groups, please speak to your regular contact at Weil, or to the contacts listed below.

**Privacy & Cybersecurity** is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this alert, or would like more information about Weil's Complex Commercial Litigation, White Collar, or Privacy & Cybersecurity practices, please speak to your regular contact at Weil, or to the attorneys listed below:

**Editors:**

| | | | |
|---|---|---|---|
| Michael Epstein (NY) | View Bio | michael.epstein@weil.com | +1 212 310 8432 |
| Randi W. Singer (NY) | View Bio | randi.singer@weil.com | +1 212 310 8152 |

**Contributing Authors:**

| | | | |
|---|---|---|---|
| Drew Tulumello (DC) | View Bio | drew.tulumello@weil.com | +1 202 682 7100 |
| Arianna Scavetti (DC) | View Bio | arianna.scavetti@weil.com | +1 202 682 7291 |
| Jason Kleinwaks (DC) | View Bio | jason.kleinwaks@weil.com | +1 202 682 7052 |