Cooley

DOJ Increases Efforts to Combat Cyber Breaches by Targeting Government Contractors

October 8, 2021

The US Department of Justice is increasing its arsenal to pursue cyber-related fraud by government contractors and grant recipients. The program, called the "Civil Cyber-Fraud Initiative," was announced by Deputy Attorney General Lisa Monaco on Wednesday. The initiative – along with other recent steps taken by the federal government – should prompt companies to be acutely aware of any areas in which their cybersecurity measures may be deficient or out of keeping with representations made in their government contracts.

Using the False Claims Act (FCA) and other civil enforcement tools, the DOJ Fraud Section plans to target companies that provide deficient cybersecurity products or services, misrepresent their cybersecurity practices or protocols, or violate obligations in their government contracts and elsewhere to monitor or report cybersecurity incidents and breaches. In her announcement, Monaco also noted that the FCA includes a unique whistleblower provision that awards individuals who report fraudulent conduct, incentivizing insiders and others to report cybersecurity incidents to the DOJ. The FCA also allows for triple damages, which means that the government can recover three times the amount of payment on a government contract that involves cyberfraud.

Monaco's announcement is the latest in a series of efforts by the government to combat cybersecurity threats, which have become increasingly prevalent in recent months. Colonial Pipeline became a household name earlier this year when the company suffered a ransomware attack that shut down its operations, affecting gas supplies along the East Coast. Colonial reported the incident to the FBI, and the government later recovered part of the ransom Colonial paid to the hackers. In announcing the recovery in June by the DOJ's Ransomware and Digital Extortion Task Force, Monaco emphasized the US will "spare no effort" in response to ransomware attacks targeting critical infrastructure.

In May, President Joe Biden issued an executive order outlining a range of initiatives to enhance cybersecurity and improve coordination and information-sharing with the private sector. Those initiatives include enhanced requirements on certain companies to collect and share data related to cybersecurity with federal government agencies and a requirement that IT service providers work with federal authorities to investigate cyber incidents.

Several bills are pending in Congress that would impose stricter reporting requirements on companies and give more power to the Cybersecurity and Infrastructure Security Agency (CISA) to investigate and regulate responses to cyberattacks. The Senate's Sanction and Stop Ransomware Act would require critical infrastructure providers to report within 24 hours after discovering a ransomware attack, even if it is only "reasonably likely" to compromise the performance of a crucial function. Other proposals in the Senate and House would permit a 72-hour reporting window and give CISA subpoena power to investigate noncompliance. Proposed updates to the Federal Information Security Modernization Act would ensure that CISA, which operates under the Department of Homeland Security, is the primary organization regulating and responding to cyberattacks.

In addition, the SEC's 4-year-old Cyber Unit has focused on targeting cyber-related misconduct, including charging companies for allegedly misleading investors by failing to disclose data breaches. As reported in a previous Cooley blog post, the SEC brought enforcement actions against two companies this summer for alleged failures to maintain adequate disclosure controls and procedures in connection with disclosing cybersecurity incidents at the companies.

What does this mean for businesses?

Preventing and rapidly responding to cyberattacks will remain a key priority for the DOJ for the foreseeable future. The recent expansion of the tools available to DOJ means that companies can expect to see increased scrutiny on their cybersecurity products and programs, their internal controls, and their assessment and reporting of potential threats and breaches. Companies may also see an increase in parallel civil and criminal investigations or multi-agency investigations (including by the FBI, SEC and CISA) relating to company

cybersecurity programs and policies.

Companies that do business with or receive government funding must ensure that their products are sufficient to prevent cyberattacks, and that they are fulfilling their obligations in their government contracts to safeguard data and maintain sufficient data security.

Other businesses should also expect increased scrutiny regarding their cybersecurity measures. The recent SEC settlements for disclosure controls violations involved a financial services company and educational services company, unrelated to government contracts. All companies should therefore proactively evaluate the strength of their cybersecurity infrastructure, including their internal monitoring and reporting processes, to identify and address potential issues before they become the subject of a government investigation.

Key Contacts

Russell Capone **New York**	**rcapone@cooley.com** **+ 1 212 479 6580**
Tiana Demas	tdemas@cooley.com +1 212 479 6560
Andrew D. Goldstein Washington, DC	agoldstein@cooley.com +1 202 842 7805
Daniel Grooms Washington, DC	dgrooms@cooley.com +1 202 776 2042
John H. Hemann San Francisco	jhemann@cooley.com +1 415 693 2038
Matthew Kutcher Chicago	mkutcher@cooley.com +1 312 881 6645

you should seek professional counsel.