Published on *The National Law Review* https://natlawreview.com

DOJ Announces Cybersecurity Enforcement Initiative Targeting Federal Contractors

Article By:

Joseph J. Lazzarotti

Jason C. Gavejian

Maya Atrakchi

Last week, the Department of Justice ("DOJ") announced the launch of its Civil Cyber-Fraud Initiative ("the Initiative") aimed at combating "new and emerging cyber threats to the security of sensitive information and critical systems" specifically targeting accountability of cybersecurity obligations for federal contractors and federal grant recipients, by way of the False Claims Act. The Initiative will be led by the Civil Division's Commercial Litigation Branch – Fraud Section.

The False Claims Act imposes liability on persons and entities that defraud governmental programs. The Initiative will hold persons and entities accountable, via the False Claims Act, for several practices related to cybersecurity practices including: 1) putting U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, 2) knowingly misrepresenting cybersecurity practices or protocols, and 3) knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

"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," said Deputy Attorney General Lisa O. Monaco in her announcement of the Initiative.

> ***Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fiscal and public trust.***

As detailed in Deputy General Monaco's announcement, benefits of implementing the Initiative will include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.
- Holding contractors and grantees to their commitments to protect government information and infrastructure.
- Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.
- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.
- Improving overall cybersecurity practices that will benefit the government, private users and the American public.

Notably, that same day, the DOJ also announced a 2nd cybersecurity related initiative, the National Cryptocurrency Enforcement Team ("the Team"), which will address activities by entities such as virtual currency exchanges that misuse cryptocurrency for criminal activity, including ransomware attacks. The Team, in addition to prosecuting such violations, will help recover lost cryptocurrency payments, including those to ransomware groups.

The DOJ is strategically increasing focus on cybersecurity, as the Biden Administration makes cybersecurity a top priority. The U.S. government has continued to ramp up efforts to strengthen its cybersecurity in the past year, and we can expect states to continue to legislate and regulate in this area. Businesses across all sectors will likely experience pressure to evaluate their data privacy and security threats and vulnerabilities and adopt measures to address their risk and improve compliance.

National Law Review, Volume XI, Number 291