SheppardMullin
Government Contracts & Investigations Blog
Latest updates on Developments Affecting Government Contracts & Investigations

DOJ Announces Civil Cyber-Fraud Initiative To Enforce Contractor Cybersecurity Compliance

By Townsend Bourne, Nikole Snyder, Lauren Weiss & Lillia Damalouji* on October 28, 2021

POSTED IN CYBERSECURITY, DEPARTMENT OF JUSTICE, FCA

On Wednesday, October 6, 2021, the Department of Justice ("DOJ") **announced** a new **Civil Cyber-Fraud Initiative** to enforce cybersecurity standards and reporting requirements. The Initiative will use DOJ's civil enforcement mechanisms, namely the False Claims Act, to pursue government contractors and federal grant recipients that "knowingly provid[e] deficient cybersecurity products or services, knowingly misrepresent[] their cybersecurity practices or protocols, or knowingly violat[e] obligations to monitor and report cybersecurity incidents and breaches." DOJ will not limit enforcement to entities; individuals also can be held accountable for cybersecurity-related fraud. Under the False Claims Act, penalties for such violations could be substantial, including treble damages.

The new Initiative is being launched following DOJ's broad review of cybersecurity threats and an extensive May 2021 Executive Order aimed at improving the Nation's cybersecurity (discussed previously **here**). Under the Executive Order, the government plans to release several new Federal Acquisition Regulation ("FAR") clauses applicable to contractors that will standardize cybersecurity rules across agencies, impose additional reporting requirements, and set standards for secure software development. Once released, contractors will need time to digest and implement these new rules.

The DOJ Initiative likely will create additional pressure for companies to devote substantial resources to cybersecurity compliance. Further, given the current environment of numerous, complex requirements that are not always clear, such uncertainty, coupled with DOJ's announcement, may lead to an uptick in whistleblower activity. Indeed, in remarks issued following announcement of the Initiative, **DOJ stated** it "expect[s] whistleblowers to play a significant role" in identifying "knowing" compliance failures and misconduct, and plans to protect and compensate whistleblowers using all available legal authorities.**[1]**

To reduce risk associated with this new Initiative, contractors should seek workable policies and strong teams dedicated to data security and the continuous monitoring of system activity. Processes for identifying and reporting cyber incidents should be developed and understood. Further, ensuring the government customer is provided with accurate and current information should reduce the likelihood a contractor will be subject to scrutiny under the newly-announced DOJ Initiative.

*Lillia Damalouji is a law clerk in the firm's Washington, D.C. office.

FOOTNOTES

[1] *See also* "Justice Official Dangles Liability Protections to Encourage Private Sector Breach Reports, available at **https://www.nextgov.com/cybersecurity/2021/10/justice-official-dangles-liability-protections-encourage-private-sector-breach-reports/186253/**
