Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Twin DOJ Initiatives Tackle Cybersecurity Fraud and Cryptocurrency Enforcement

October 11, 2021

Key Points

- On October 6, 2021, the DOJ announced two new initiatives: the Civil Cyber-Fraud Initiative and the National Cryptocurrency Enforcement Team.
- The Civil Cyber-Fraud Initiative will fight rising cyber threats to government contractors and grant recipients. This initiative will involve enforcement of the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients to penalize entities and individuals that knowingly provide deficient cybersecurity, misrepresent their cybersecurity practices, or violate their obligations to report incidents and data breaches.
- The newly created National Cryptocurrency Enforcement Team will pursue prosecutions against cryptocurrency exchanges and other entities that enable the misuse of cryptocurrency to commit criminal activity, such as money laundering or the receipt of ransomware payments. The team will also help to recover cryptocurrency lost to fraud and extortion, including payments to ransomware groups.

Background

On October 6, 2021, the Department of Justice (DOJ) announced twin programs focusing on monitoring contractor cybersecurity, and combating cryptocurrency used for illicit purposes. This announcement is part of DOJ's strategic cyber threat review, and follows a series of well-publicized cyber incidents and subsequent federal efforts to shore up security among government agencies and contractors.

In December of last year, a cyberattack exploited a flaw in a product produced by third-party software provider SolarWinds, which caused a breach in several federal agency networks.[1] Similar supply chain focused cyberattacks occurred this year, including the May attack on fuel supplier Colonial Pipeline. On May 12, 2021, President Biden issued an Executive Order (EO 14.028) focusing on revamping supply chain cybersecurity, particularly for government contractors and software providers (read more about the EO in our previous post here). The effort builds on other related initiatives, including Section 889 and the Commerce Department's information and

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

James Joseph Benjamin Jr.
Partner
jbenjamin@akingump.com
New York
+1 212.872.8091

Ian Patrick McGinley
Partner
imcginley@akingump.com
New York
+1 212.872.1047

Michael Asaro
Partner
masaro@akingump.com
New York
+1 212.872.8100

Peter Altman
Partner
paltman@akingump.com
Los Angeles
+1 310.728.3085

Michael J. Vernick
Partner
mvernick@akingump.com
Washington, D.C.
+1 202.887.4460

communications technology and services (ICTS) supply chain regulations. Most notably, in relation to the October 6 announcement, the May 12 EO builds on nearly a decade of progress toward establishing cybersecurity and incident reporting standards for federal contractors under the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), including through the Department of Defense's (DOD) recent efforts to establish a Cybersecurity Maturity Model Certification (CMMC) and formalize a cybersecurity assessment and scoring framework. Contractors should look to recent rulemakings implementing these assessments and frameworks, which we described in our fall 2020 webinar here, as well as regulations implementing Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019), described here. Further information on the DOD's CMMC program can be found in our previous post here. The Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) followed the May 12 EO with draft guidance to implement a "Zero-Trust cybersecurity policy." Although this guidance is aimed at federal agencies, it has implications for government contractors, as well, promoting cybersecurity with zero-trust architecture (read more about Zero-Trust policy here).

In response to the Colonial Pipeline ransomware attack and other well-publicized ransomware attacks, DOJ has also enhanced its response to cyber threats. In June, DOJ created a Ransomware and Digital Extortion Task Force to centralize and enhance prosecutions of ransomware groups.[2] In August, DOJ announced the creation of a Cyber Security Fellows program, a three-year program designed to train new prosecutors to handle ransomware and cryptocurrency related crimes.[3] The new programs announced on October 6 underscore the prominence of cybersecurity as a federal concern, and the willingness of DOJ to use both criminal and civil tools to hold bad actors accountable.

What the Civil Cyber-Fraud Initiative Means for Federal Contractors and Grant Recipients

According to the announcement, the Civil Cyber-Fraud Initiative ("the initiative") will use the existing False Claims Act (FCA) against government contractors and grant recipients that fail to implement sufficient cybersecurity protections. The FCA is a civil tool long used by the government to redress fraudulent claims for federal funds and includes provisions encouraging whistleblowers to identify possible FCA violations by allowing them to share in any recovery. In relation to the FCA, the initiative will hold companies accountable for the following:

- Knowingly providing deficient cybersecurity products or services.
- Knowingly misrepresenting cybersecurity practices.
- Knowingly violating obligations to monitor and report cybersecurity incidents and breaches.[4]

The first stated benefit of the initiative is "building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners."[5] Other benefits listed similarly emphasize the importance of promoting strong cybersecurity policies by government contractors, with potential FCA cases providing motivation.

Angela B. Styles
Partner
astyles@akingump.com
Washington, D.C.
+1 202.887.4050

Chris Chamberlain
Title (Sidebar text, Arial 9pt)
cchamberlain@akingump.com
Washington, D.C.
+1 202.887.4308

The National Cryptocurrency Enforcement Team

The National Cryptocurrency Enforcement Team (NCET) is DOJ's attempt to target the lifeblood of cybercrime by pursuing illegal cryptocurrency uses. The announcement states that NCET members will be largely drawn from DOJ's Money Laundering and Asset Recovery Section (MLARS), Computer Crime and Intellectual Property Section (CCIPS) and Assistant U.S. Attorneys from across the country. These team members will pursue cases against entities that "enable the misuse of cryptocurrency and related products to commit or facilitate criminal activity."[6] According to the announcement, the NCET will also take on a support role for federal, state, local and international law enforcement authorities that tackle cryptocurrency related crime.

The announcement lists the NCET's primary targets as: cryptocurrency exchanges, mixing and tumbling services (which mix identifiable cryptocurrency funds with others to prevent tracing), and money laundering infrastructure providers. The NCET will investigate and prosecute fraudulent misuse of cryptocurrency, illegal laundering and other illegal uses of cryptocurrency by these entities and others.

Takeaways

These twin initiatives indicate that cybersecurity remains a top federal priority and one likely to grow in importance in the coming years. DOJ is using its enforcement powers to incentivize businesses, both government contractors and cryptocurrency exchanges, to stop illegal activity before it happens. This suggests that DOJ is expanding its focus from prosecuting individual bad actors, to initiating civil and criminal actions against the gatekeepers and facilitators of cybercrime. In the cryptocurrency space, this means that operators of exchanges will likely face enhanced scrutiny by DOJ, as DOJ continues to target the misuse of cryptocurrency to facilitate criminal conduct.

In addition, private entities working with government information systems are now considered part of the cyber defense apparatus. Criminal and civil cases in this area are likely to increase, and companies, especially federal contractors, would be well advised to review their cybersecurity and anti-money laundering policies. Up-to-date cybersecurity practices, comprehensive incident reporting policies and strong monitoring practices are vital components in conducting business with the government.

[1] CISA Issues Emergency Directive to Mitigate the Compromise of SolarWinds Orion Network Management Products, Cybersecurity and Infrastructure Agency (December 13, 2020) available at https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network.

[2] U.S. Dept. of Justice, *Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion*, Memorandum (June 3, 2021) available at https://www.justice.gov/dag/page/file/1401231/download.

[3] U.S. Dept. of Justice, *Deputy Attorney General Lisa Monaco Announces Creation of New Cyber Fellows Positions* (August 27, 2021) available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-monaco-announces-creation-new-cyber-fellows-positions.

[4] U.S. Dept. of Justice, *Deputy Attorney General Lisa O. Manaco Announces New Civil Cyber-Fraud Initiative* (October 6, 2021) available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[5] *Id*. at 1.

[6] U.S. Dept. of Justice, *Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team* (October 6, 2021) available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.