David J. Kappos
+1-212-474-1168
dkappos@cravath.com

Rachel G. Skaistis
+1-212-474-1934
rskaistis@cravath.com

Minh Van Ngo
+1-212-474-1465
mngo@cravath.com

John D. Buretta
+1-212-474-1260
jburetta@cravath.com

Benjamin Gruenstein
+1-212-474-1080
bgruenstein@cravath.com

David M. Stuart
+1-212-474-1519
dstuart@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

U.S. Securities and Exchange Commission 2019 Budget Request Prioritizes Cybersecurity Enforcement and Management of Internal Cybersecurity Risk

February 14, 2018

On Monday, the U.S. Securities and Exchange Commission announced that it had requested a $1.66 billion budget for the 2019 fiscal year, an increase of 3.5% over the prior year's request. Compared to the FY 2018 budget request, which mentions cybersecurity only once in passing, the new budget request reflects a notably increased focus on strengthening the Commission's cybersecurity enforcement efforts and supporting enhancements to its technology systems and broader risk program. The SEC's budget request is included in the Congressional Budget Justification and is available at sec.gov.

CYBERSECURITY ENFORCEMENT

Building on a number of cyber-related initiatives and enforcement actions announced since SEC Chairman Jay Clayton was sworn in last spring, the SEC's new budget request provides yet another indication that cybersecurity will be one of the most important enforcement priorities for the Commission in the near future. In fact, the request lists "combatting cyber-related threats" as one of the two key priorities for the SEC's Enforcement Division, reflecting a trend that has been growing for months.

On September 25, 2017, the SEC announced the creation of a Cyber Unit to enhance its ability to "detect and investigate cyber threats through increasing expertise in an area of critical national importance". The Cyber Unit is focused on bringing enforcement actions against actors involved in what it describes generally as "cyber-related misconduct", including hacking to obtain material nonpublic information, schemes to spread false information through social media, threats to trading platforms and violations involving distributed ledger technology and initial coin offerings (ICO).

According to the SEC, the requested budget increase will provide added resources to support and expand the work the Cyber Unit has already begun. On December 4, 2017, the Cyber Unit announced that it had filed its first charges against PlexCorps, a Canadian company, as well as its principal executive and his partner. According to the SEC's complaint, filed in the U.S. District Court for the Eastern District of New York, the defendants launched a purported ICO in which they offered "PlexCoin" tokens and promised investors massive returns in what the SEC alleges was a fraudulent and unregistered offering of securities. In its press release announcing the charges, the SEC emphasized its quick work to obtain an emergency asset freeze to halt the ICO.

One week later, the SEC Cyber Unit announced that a California-based company had voluntarily agreed to halt its ICO after it was contacted by the Cyber Unit. The company, Munchee Inc., had been selling digital tokens to investors to raise capital for its blockchain-based food review service. By agreeing to stop the ICO, immediately returning proceeds before issuing the tokens and cooperating with the investigation, the company avoided imposition of a penalty, though it did agree to an order in which the SEC found that its conduct constituted unregistered securities offers and sales.

Most recently, on January 30, 2018, the SEC announced that the Cyber Unit assisted in an investigation that resulted in a court order halting an allegedly fraudulent ICO by Dallas-based AriseBank. According to the Commission, AriseBank and its principals sought to raise hundreds of millions from investors by misrepresenting the company as a first-of-its-kind "decentralized bank" offering its own cryptocurrency to be used for a broad range of customer products and services.

MANAGEMENT OF INTERNAL CYBERSECURITY RISK

In addition to the expansion of enforcement actions responding to cyber-enabled misconduct, the increased budget request also reflects the SEC's recognition of its need to implement enhancements to protect the security of its network, systems and sensitive data. The budget request comes less than five months after the Commission revealed that the Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system, its electronic filing system for public company disclosures, was hacked in 2016. The intrusion was disclosed to the public in a lengthy statement issued by Chairman Clayton on September 20, 2017 that, among other things, acknowledged that the breach may have allowed for illicit gain through trading.

In an updated statement issued on October 2, 2017, Chairman Clayton disclosed that further review and investigation of the breach revealed that an EDGAR test filing accessed by third parties as a result of the intrusion contained personal information of two individuals. In an effort to address the concerns that would follow, the SEC indicated in its press release that it had added, and expected to continue to add, additional resources to efforts to modernize the EDGAR system. The 2019 budget request should provide for at least part of the additional resources necessary for the Commission to be able to continues these efforts, which are critical for the agency as it seeks to focus its energies on enforcement rather than the state of its internal defenses. These resources include additional staff positions as well as tools, technologies and services to enable the Commission to expand its cybersecurity defenses, particularly with regard to incident management and response, advanced threat intelligence monitoring and enhanced database and system security.

CONCLUSION

With the requested budget increase for 2019, the SEC has made clear that two important priorities for Chairman Clayton's tenure relate to the area of cybersecurity. First, investors are likely to see more cyber-related enforcement actions generally and in the area of ICOs and digital currencies in particular. Second, the SEC is implementing a much-needed effort to upgrade its own cybersecurity risk profile. The SEC is sending a clear signal that it hopes to continue to play a critical enforcement role in protecting investors from cyber threats, while at the same time restoring the faith of investors and regulated entities in its ability to protect their data responsibly.

New York
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

London
CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

www.cravath.com