Articles + Publications | March 21, 2025

4 Actions for Cos. as SEC Rebrands Cyber Enforcement Units

WRITTEN BY

Sadia Mirza | Casselle A.E. Smith | Charlene C. Goldfield | Jay A. Dubow | David I. Meyers | Ghillaine A. Reid

On Feb. 20, the U.S. Securities and Exchange Commission announced the creation of the Cyber and Emerging Technologies Unit, which will replace the Enforcement Division's previous Crypto Assets and Cyber Unit.[1]

The SEC stated that the CETU will focus on combating online misconduct and protecting retail investors from bad actors in the emerging technology space. The newly constituted CETU will be led by Laura D'Allaird, former co-chief of the Crypto Assets and Cyber Unit.

This marks the second major shift for the unit, which was originally established in 2017 during the first Trump administration as the Cyber Unit. In 2022, under the leadership of former SEC Chair Gary Gensler, the unit was renamed the Crypto Assets and Cyber Unit to encompass crypto-assets and nearly doubled in size from 30 to 50 dedicated positions.[2]

In announcing the CETU's creation last month, the SEC stated that the headcount has been reduced back down to 30 and that it "will complement the work of the Crypto Task Force led by Commissioner Hester Peirce." The Crypto Task Force, which was launched on Jan. 21 by acting Chair Mark T. Uyeda,[3] sits outside the SEC's Enforcement Division.

As Uyeda explained in a Feb. 24 speech, the Crypto Task Force "will seek to develop a comprehensive regulatory framework to provide realistic paths to registration and to craft sensible disclosure frameworks."[4] According to Uyeda in the Feb. 20 press release announcing the creation of the CETU, this restructuring "will allow the SEC to deploy enforcement resources judiciously."

The SEC announced that the CETU will focus on seven priority areas. Consistent with its new name, the CETU is shifting its focus beyond cryptocurrency to include issues such as artificial intelligence and other emerging technologies, which in addition to posing risks may be exploitable by bad actors to deceive investors.

Three of the seven key areas where the CETU will specifically target fraudulent activities, include emerging technologies, are "fraud committed using emerging technologies, such as artificial intelligence and machine learning; use of social media, the dark web, or false websites to perpetrate fraud; … [and] fraud involving blockchain technology and crypto assets." This likely signals a shift away from the previous administration's

pursuit of nonfraud registration cases concerning digital assets.

The other four key areas that the SEC intends to prioritize involve cyber-related misconduct, specifically "hacking to obtain material nonpublic information," which can be used to facilitate illegal trading; "takeovers of retail brokerage accounts; … regulated entities' compliance with cybersecurity rules and regulations; and "public issuer fraudulent disclosure relating to cybersecurity."

Notably, three of these four areas focus on the conduct of cybersecurity threat actors, as opposed to the companies that fall victim to their malicious attacks. This should be a welcome improvement for public companies that viewed many of the SEC's recent cybersecurity enforcement actions as blaming the victim and punishing companies that disclosed material cybersecurity incidents in their public filings.

Although not explicitly stated, the reference to "cybersecurity rules and regulations" likely pertains to the enforcement of the SEC cybersecurity risk management rules promulgated in 2023.[5] However, it may also signal a retreat from the prior administration's expansive approach to cybersecurity enforcement for public companies. As we discussed last year, the Crypto Assets and Cyber Unit has sought to expand the SEC's rules regarding internal accounting controls by including cybersecurity in that category.[6]

Clearly, numerous changes were to be anticipated with the presidential transition from President Joe Biden to President Donald Trump. The creation of the CETU may be just one of the many outcomes from this executive administration's approach to securities regulation. As Uyeda noted during his Feb. 24 remarks at the Florida Bar's 41st Annual Federal Securities Institute and M&A Conference, "the Commission has begun the process of returning to its narrow mission to facilitate capital formation, while protecting investors and maintaining fair, orderly, and efficient markets."[7]

Though the SEC is significantly curtailing its enforcement regime in the crypto space, the Division of Enforcement's cybersecurity program appears poised for the long haul. Public companies, and specifically financial institutions and technology companies, should consider the following key takeaways.

1. Implement or strengthen compliance regimes.

The CETU's aim is to concentrate on other emerging technologies that have been shaping business. Artificial intelligence and machine learning will probably be a focus of the CETU as more agencies such as the SEC examine how these technologies affect the day-to-day experiences of American citizens.[8]

Data analytic companies, investment advisers or other SEC-regulated entities that utilize artificial intelligence as part of their stock market analysis or trading should ensure that they are implementing or updating compliance programs that incorporate the latest regulatory requirements.

2. Emphasize cybersecurity reporting and disclosure.

The new administration is maintaining its focus on addressing cyber-related misconduct. There remains a strong emphasis on ensuring that investors are well informed about cybersecurity risks and incidents concerning the companies they invest in. Additionally, the SEC has renewed its focus on targeting hackers who gain unauthorized

access to material nonpublic information, which could be used to facilitate illegal trading.

Considering these priority areas, businesses would be prudent to take the following steps.

Review incident response plans and materiality assessment procedures.

Ensure that these plans and procedures align with the SEC's rules on reporting material incidents. This includes adhering to the SEC's May 2024 guidance on disclosing "other cybersecurity incidents" through the use of Item 8.01 on Form 8-K.[9] This provision allows companies to disclose a cybersecurity incident for which they have not yet made a materiality determination or that they determined to be nonmaterial.

Pay attention to incidents potentially affecting MNPI.

Review the processes for assessing materiality and categorizing incidents within the incident response plan. Pay particular attention to incidents that may implicate MNPI, as these could affect the materiality profile of an incident.

While the CETU's priority areas suggest that the primary targets of enforcement actions related to unauthorized access to MNPI are the hackers themselves, companies that experience incidents involving MNPI but fail to report them, or do not report them in a timely manner, may face similar consequences.

Review prior risk factors and disclosures.

Conduct a thorough review of prior risk factors and disclosures to ensure they are up to date. For example, if a company's SEC filings outline potential challenges and adverse conditions that could arise from a cybersecurity incident, an investor might incorrectly assume that no incident has occurred if the disclosures are not updated.

Ensuring that disclosures accurately reflect the current situation helps maintain transparency and prevents the misleading of investors about the company's cybersecurity status.

3. Crypto-asset businesses should heed to continuous and sound legal advice.

While this administration is open to a more crypto-friendly environment, it is unclear how the SEC or the White House will approach crypto regulation. This uncertainty can prove challenging, so crypto-asset entities should still ensure that they are conducting business within the legal frameworks that currently exist.

Entities engaging in the crypto-asset business should continue to monitor their obligations under the SEC and incorporate compliance programs that promote antifraud business practices and abide by all policies and regulations.

4. Be open to regulatory harmonization.

A broader framework imposed on the CETU could signal a focus on more regulatory harmonization. Companies should take this opportunity to engage with the SEC to help shape policy surrounding regulatory oversight of these key emerging technology areas.

[1] SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors, SEC.gov | SEC Announces Cyber and Emerging Technologies Unit to Protect Retail Investors, https://www.sec.gov/newsroom/press-releases/2025-42.

[2] SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit, SEC.gov | SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit, https://www.sec.gov/newsroom/press-releases/2022-78.

[3] SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force, SEC.gov | SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force, https://www.sec.gov/newsroom/press-releases/2025-30.

[4] Remarks at the Florida Bar's 41st Annual Federal Securities Institute and M&A Conference, SEC.gov | Remarks at the Florida Bar's 41st Annual Federal Securities Institute and M&A Conference, https://www.sec.gov/newsroom/speeches-statements/uyeda-remarks-florida-bar-022425.

[5] Troutman Pepper Locke, "SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on Their Security and Disclosure Plans," https://www.troutmanfinancialservices.com/2023/07/sec-adopts-final-cybersecurity-rules-requires-companies-to-focus-on-their-security-and-disclosure-plans/.

[6] Troutman Pepper Locke, "SolarWinds Ruling Offers Cyber Incident Response Takeaways," https://www.troutman.com/insights/solarwinds-ruling-offers-cyber-incident-response-takeaways.html.

[7] Remarks at the Florida Bar's 41st Annual Federal Securities Institute and M&A Conference, SEC.gov | Remarks at the Florida Bar's 41st Annual Federal Securities Institute and M&A Conference, https://www.sec.gov/newsroom/speeches-statements/uyeda-remarks-florida-bar-022425.

[8] Office of the Strategic Hub for Innovation and Financial Technology (FinHub), SEC.gov | Office of the Strategic Hub for Innovation and Financial Technology (FinHub), https://www.sec.gov/about/divisions-offices/office-strategic-hub-innovation-financial-technology-finhub.

[9] Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, https://www.sec.gov/newsroom/speeches-statements/gerding-cybersecurity-incidents-05212024.

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations
- Privacy + Cyber