U.S. COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-6700
Facsimile: (202) 418-5407
jsterling@cftc.gov

Division of Swap Dealer and
Intermediary Oversight

Joshua B. Sterling
Director

TO: CFTC Registrants

FROM: Joshua B. Sterling, Director
Division of Swap Dealer and Intermediary Oversight

DATE: March 19, 2020

RE: Cybersecurity during Coronavirus (COVID-19) Alert

As registered participants in the markets the CFTC oversees, we recognize that you must react to unexpected events, like COVID-19 (coronavirus), that potentially impact your legal and regulatory obligations. Many CFTC registrants have expanded the use of telework to facilitate social distancing and minimize the spread of the virus. Given the increase in telework, the following cybersecurity resources may be helpful:

- On March 13, 2020, the Cybersecurity and Critical Infrastructure Agency (CISA) of DHS issued Awareness Alert AA20-073A,[1] "Enterprise VPN Security," to advise organizations of cybersecurity considerations and mitigations for enterprise virtual private network (VPN) solutions enabling teleworking employees to connect to an organization's information technology (IT) network. As organizations implement telework, CISA encourages them to adopt a heightened state of cybersecurity.
- On March 6, 2020, CISA issued a Cyber Alert,[2] "Defending Against COVID-19 Cyber Scams," reminding individuals to remain vigilant for scams related to COVID-19. Cyber actors have been sending emails with malicious attachments or links to fraudulent websites attempting to trick recipients into revealing sensitive information or donating to fraudulent charities or causes. Organizations are encouraged to caution staff and customers in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19. Such cautions are particularly important for both market participants and their employees in a teleworking context.
- On March 6, 2020, CISA issued a CISA Insights document,[3] "Risk Management for Novel Coronavirus (COVID-19)," outlining physical, supply chain, and cybersecurity issues that may arise from the spread of COVID-19. As organizations explore various alternate workplace options in response to COVID-19, CISA recommends examining the security of information technology systems by taking the following steps:
    - Secure systems that enable remote access.
        - Ensure VPN and other remote access systems are fully patched.

        - Enhance system monitoring to receive early detection and alerts on abnormal activity.
        - Implement multi-factor authentication.
    - Ensure all machines have properly configured firewalls, as well as anti-malware and intrusion prevention software installed.
    - Test remote access solutions capacity, and increase capacity, as necessary.
    - Ensure continuity of operations plans or business continuity plans are current.
    - Increase awareness of information technology support mechanisms for employees who work remotely.
    - Update incident response plans to consider workforce changes in a distributed environment.

  The document also provides recommendations for infrastructure protection and managing supply chain risks.

- On March 6, 2020, the FFIEC issued a press release,[4] "FFIEC Highlights Pandemic Preparedness Guidance," updating guidance identifying actions that financial institutions should take to minimize the potential adverse effects of a pandemic. Supervised institutions should periodically review related risk management plans, including continuity plans, to ensure their ability to continue to deliver products and services in a wide range of scenarios and with minimal disruption. More information about financial institution cybersecurity is available from the FFIEC at https://www.ffiec.gov/cybersecurity.htm.

Registrants are also encouraged to notify law enforcement of any cyber activity targeting the institution or its customers.

If you have questions, please do not hesitate to contact DSIO staff: Barry McCarty, Special Counsel, at CMcCarty@cftc.gov or Helene Schroeder, Special Counsel, at HSchroeder@CFTC.gov or DSIOCyberAlerts@CFTC.gov.

[1] https://www.us-cert.gov/ncas/alerts/aa20-073a
[2] https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams
[3] https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf
[4] https://www.ffiec.gov/press/pr030620.htm