RIVELES WAHAB LLP INFO@RANDWLAWFIRM.COM | 212-785-0076 | www.RANDWLAWFIRM.com
40 WALL STREET, FLOOR 28, NY, NY 10005

CFTC Approves NFA Cybersecurity Interpretive Notice

Acknowledging the rapid evolution of information technology and correspondent threats, on August 20, 2015 the National Futures Association ("NFA") issued an Interpretive Notice addressing cybersecurity concerns. The Interpretive Notice established general requirements relating to the information systems security programs ("ISSPs") of futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants (collectively, "Members"). The Commodities Futures Trading Commission ("CFTC") recently approved the Interpretive Notice, which will become effective on March 1, 2016 and will apply to all Members.

Recognizing the diversity of its Members and the fluid nature of cybersecurity threats, the NFA is providing Members broad discretion to design and implement ISSPs. Members are encouraged to tailor their ISSPs, and each Member should take into account (1) the size and complexity of its operation, (2) the types of customers and counterparties it serves, and (3) its electronic interconnectivity with other entities.

While flexibility is the hallmark of this Interpretive Notice, it does mandate certain program components. Specifically, Member ISSPs must include:

Written Program: Each Member must adopt a written ISSP, reasonably designed to provide safeguards against cybersecurity threats. In designing the program, Members should consider the aforementioned operation-specific factors. The written ISSP must be approved, in writing, by the Member's Chief Executive Officer, Chief Technology Officer, or other executive level official. If applicable, the Member's senior management team should periodically provide information about the ISSP to the Member's board of directors (or similar body).

Security and Risk Analysis: Members have an ongoing obligation to evaluate and analyze the risks associated with their technology systems. The Interpretive Notice specifically requires that Members: (1) maintain an inventory of critical informational technology hardware and software; (2) identify and manage the significant internal and external threats and vulnerabilities to at-risk data, including customer data, corporate records, and financial information; (3) assess the threats to and vulnerability of their electronic infrastructure and the threats and vulnerabilities posed through applicable third-party service providers; and (4) know the devices connected to their network and network structure.

In performing the required evaluations, Members should remain cognizant of past, present, and future risks. Members must estimate the severity of potential threats, perform a vulnerability analysis, and analyze their prior security incidents. If appropriate, firms should assign personnel from their business, information technology, back-office, risk management, or internal audit teams to perform the required analyses.

Deployment of Protective Measures: Members must adopt, document, and describe specific safeguards to protect against the threats identified in their security and risk analysis. These protective measures, like other aspects of the ISSPs, will be Member-specific and should be designed in contemplation of the Member's size, business, technology, interconnectivity with third parties, and particular risks. Members should also adopt procedures to detect unidentified, ongoing potential threats. To this end, Members are encouraged to monitor their physical premises and technological networks in order to prevent unauthorized access.

Response and Recovery Plan: A Member's ISSP must contain an incident response plan, which will guide Member personnel in the event of a security breach. The plan should include procedures for assessing and mitigating damage and a plan for communicating the breach with internal and external authorities. Members are also encouraged to form an incident response team responsible for coordinating the investigation and response.

Employee Training: The ISSP should also outline the Member's ongoing education and training programs. Appropriate employees should undergo this training upon hire and periodically throughout the course of their employment

Ongoing Responsibilities: Once a Member has designed and implemented its written ISSP, it must continuously monitor, review, and adjust the program. Reviews must be performed at least annually, and may be conducted by in-house staff or independent third-party specialists. Members must also remain cognizant of the risks posed by outside service providers and, to the extent possible, perform due diligence on critical service providers and avoid providers with substandard security practices. Finally, Members must maintain all records related to their ISSPs in accordance with NFA compliance regulations.