crowell moring

CLIENT ALERT

The NFA Weighs In With New Cybersecurity Guidance

Oct.02.2015

The National Futures Association (NFA) has proposed a new interpretive notice (Proposed Notice) to the Commodity Futures Trading Commission (CFTC) which contains the NFA's standards for Information Systems Security Programs (ISSPs). While the requirement to have an ISSP is not new, the Proposed Notice puts another tool in the NFA's examination toolbox, allowing it to assess penalties for failure to have a conforming ISSP. The Proposed Notice also provides regulatory personnel with a roadmap for compliance.

The Proposed Notice applies to all Futures Commission Merchants, Retail FX Dealers, Commodity Trading Advisers, Commodity Pool Operators, Introducing Brokers, Swap Dealers and Major Swap Participants (Regulated Entities) that are NFA registrants. But all Regulated Entities, even those that are not NFA registrants, are required by CFTC Regulation 160.30 to adopt "policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." Thus, even unregistered firms should find the compliance roadmap set out in the Proposed Notice instructive. Regulated Entities that are part of an affiliated group can use a parent entity's ISSP, but should be aware that the NFA will review the parent's ISSP against the standards set out in the Proposed Notice subject to the type, size and complexity of the group's operations.

In many cases, Regulated Entities are subject to the rules of the Securities Exchange Commission (SEC) as well. In practice, one ISSP should be able to satisfy the requirements of the CFTC and NFA as well as the SEC, but firms should confirm that both their futures business and their securities business comply with the policy's terms. Our previous alerts on the SEC's guidance can be found here and here.

While a strong ISSP cannot prevent all security breaches, a robust set of policies and procedures that are carefully followed will likely be a factor considered by regulators in assessing penalties both in the event of a breach and in regular examinations.

What should Regulated Entities do next?

- **Develop an ISSP, or check that current ISSPs conform to generally accepted standards**.
    - The NFA suggests a number of third-party resources that are useful in developing security policies. For example, the National Institute for Standards and Technology (NIST) has released a detailed framework which refers organizations to what NIST considers the best of the industry-created provisions for each facet of an ISSP. The Proposed Notice also references for review standards promulgated by SANS, the Open Web Application Security Project (OWASP) and the Control Objectives for Information and Related Technology (COBIT).
    - As part of the program, Regulated Entities have an obligation to conduct a security and risk analysis, deploy protective measures against identified threats and vulnerabilities, and develop a response and recovery incident plan.

  - One relatively new trend among the procedures the NFA recommends is the use of application whitelists, which prevent any unauthorized software from operating on a computer system. Other recommendations include physical and electronic access controls, use of supported and updated software, regularly backing up systems (which should be addressed in a firm's disaster recovery plan as well), and using web filtering technology to block access to potentially malicious websites.
  - An ISSP should identify who is responsible for compliance with various aspects of the policy – for example, who is responsible for initiating and conducting periodic reviews, who must be contacted to conduct diligence of a vendor before that vendor is onboarded, and who will serve on an emergency team to respond rapidly to security incidents.
  - No ISSP is complete without an incident response plan. Among other things, an incident response plan should include emergency contact information for the emergency response team (which should be communicated to all employees and vendors), internal escalation procedures, identification of parties required to be notified of any security breach (including regulatory authorities, law enforcement, customers, and employees), a description of the relevant information to be delivered to each such party, and procedures for investigation of breaches (including the use of an outside vendor to investigate, if desired).
- **Ensure management review and approval in writing**. The Proposed Notice requires that a NFA registrant's ISSP be approved in writing by the registrant's CEO, CTO or another executive-level officer, and states that management should provide information about the ISSP to the board of directors. Discussions about the ISSP at the board level should be documented in board minutes, which should be available for review by the NFA in exams. Even for non-registrants, involving management and directors in information security fosters a culture of compliance and can help demonstrate that information security is understood as a duty of care.
- **Conduct periodic review of the ISSP**. The NFA recommends that ISSPs be reviewed every 12 months. This review should include vulnerability assessments (both consideration of the firm's critical infrastructure and weaknesses, identification of the types of information that need to be protected, a review of recent security breaches affecting other firms), consideration of product developments in the world of cybersecurity, and a tabletop or dry run exercise to test the effectiveness of the incident response plan using hypothetical scenarios. Upon the conclusion of a review, the CEO, CTO or another executive-level officer should reapprove the policy (even if it has not changed), and the board should receive an update documented in board minutes.
- **Ensure security of information held by third party service providers**. If a vendor will have access to protected information, that vendor's contract should include provisions requiring the vendor to ensure the security of that information. In addition, Regulated Entities should conduct due diligence of vendors which have access to protected information, including reviewing vendors' security policies and infrastructure. This due diligence should be updated annually, and records should be kept of the results.
- **Conduct periodic employee training**. The NFA recommends that employees be trained at the time they are hired, and receive annual refresher training.
- **Conduct independent testing of security systems**. The CFTC recommends that independent testing be conducted every two years. Regulated Entities should maintain documentation of the results of such testing, and should also document how the results were used in the review and update of the entity's ISSP.
- **Consider cyberinsurance**. While the Proposed Notice does not mention cyberinsurance, FINRA's recent report on cybersecurity mentioned it as another proactive measure companies can take. Although regulators will not view

cyberinsurance as a substitute for a robust ISSP, it is generally helpful in demonstrating commitment to security. Additionally, cyberinsurance may be an effective tool for an organization to help it protect its assets.

- **Join an information sharing organization**. Organizations such as the Information Sharing and Analysis Organizations (ISAOs) and the Information Sharing and Analysis Centers (ISACs) provide up-to-date information about cyberthreats, which can be used to inform a firm's ISSP.
- **Maintain records**. NFA registrants must retain records relating to their ISSPs pursuant to NFA Rule 2-10. It is a sound policy for all Regulated Entities to maintain ISSP-related records to show a history of compliance in the event that an audit or a security breach occurs. Records should be kept of all activities regarding the ISSP, including management and board review and approval, periodic reviews and updates, vendor due diligence, employee training, and independent testing.

The Proposed Notice acknowledges that many smaller NFA registrants may not have ISSPs in place that conform to its requirements, and that the NFA plans to develop an "incremental, risk-based examination approach" for smaller IBs, CPOs and CTAs. The NFA also suggests that it may provide additional, more detailed guidance in the future – registrants should continue to monitor NFA communications for additional information.

The NFA's Proposed Notice can be found here. The CFTC also issued a staff advisory last year which contains some helpful best practices for ISSPs, which can be found here.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.