NFA’s Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 entitled Information Systems Security Programs (Interpretive Notice), effective March 1, 2016, requires all Member firms to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems. To assist Members as they develop and implement their ISSPs, NFA held three Cybersecurity Workshops in February. Listen to the audio from the Chicago workshop.

During the workshops and via email, NFA has received numerous questions. In response, NFA compiled a list of answers to frequently asked questions to help Members.

1. Can I implement an ISSP on an enterprise wide basis?
Yes. NFA’s Interpretive Notice is intended to provide Members with the flexibility necessary to adopt an ISSP across a family of firms as long as the requirements outlined in the Interpretive Notice are addressed for the Member firm, including the obligation to review the ISSP once every 12 months, and the specific business activities of the Member are considered.

2. Does the ISSP need to be a single document?
No. The Interpretive Notice is intended to provide Members with the flexibility to adopt an ISSP that fits the structure of the Member’s operations, which may result in the ISSP containing multiple documents or cross-references to other underlying documents/functions that address the specific requirements outlined in the Interpretive Notice.

3. Does NFA have a preferred template for creating an ISSP?
No. Members are required to create and adopt an ISSP that addresses the relevant risks attributable to the Member. The Member must perform a risk assessment and respond to the identified risks accordingly.

4. If I already have written supervisory procedures to comply with other domestic or foreign regulators’ cybersecurity requirements, do I need to create a separate ISSP for NFA?
No. However, the Member must ensure that the written supervisory procedures address the specific requirements outlined in the Interpretive Notice, and the Member bears the burden of establishing that its ISSP satisfies the Interpretive Notice’s requirements.

5. Must I submit my ISSP to NFA?
While Members must have their written ISSP in place by March 1, Members should not submit the ISSP to NFA. NFA intends to review Members’ ISSPs during the normal course of our examination program.
6. How do I evidence my risk assessment?

The Interpretive Notice allows a Member to determine the most appropriate method for both performing and documenting its own risk assessment. The Member must be able to provide documentation supporting its assessment, which should include, but is not limited to, lists of critical hardware, software, network connections, databases, etc., used by the Member; identification of threats to sensitive information, including personally identifiable information; and classification of vulnerabilities in the Member’s technology infrastructure.

7. Can a committee approve my ISSP?

A Member’s ISSP should be approved in writing by the Member’s Chief Executive Officer, Chief Technology Officer, or other executive level official. Any committee approving the ISSP must include one of these individuals.

8. How do I evidence approval of my ISSP?

While NFA’s Interpretive Notice does not prescribe a specific method for approving the ISSP, a Member could obtain formal signature(s), retain minutes from meetings approving the ISSP, or preserve other electronic communications approving the ISSP.

9. Must I appoint a Chief Information Security Officer or equivalent?

No. However, a Member should ensure it has the expertise to perform the process necessary to develop and implement an ISSP, as well as to carry out the functions adopted in the ISSP.

10. Must I perform penetration or intrusion testing?

No. Under the Interpretive Notice the Member must determine if the ISSP is effective. To make this determination, the Member may consider penetration or intrusion testing along with other reasonable means, which include, but are not limited to, completion of NFA’s Self-Examination Questionnaire, assessment of prior cybersecurity breaches, and consideration of other known cybersecurity events occurring externally. Further, as the Interpretive Notice provides, under appropriate circumstances, a Member’s review may include penetration testing of the firm’s systems, the scope and timing of which is highly dependent upon the Member’s size, business, technology, its electronic interconnectivity with other entities and the potential threats identified in its risk assessment.

11. Will NFA perform penetration or intrusion testing?

No. NFA’s examinations will focus on the review of the Member’s ISSP to ensure that the ISSP complies with the Interpretive Notice’s requirements.
12. Does NFA recommend any particular consultants that can help a Member draft an ISSP or perform penetration testing?

No. NFA does not recommend or maintain a list of preferred service providers. The Interpretive Notice does identify a number of resources available to Members. Additionally, the following organizations may have useful resources for Members in creating ISSPs:

- The CERT Division of the [Software Engineering Institute (SEI)](https://www.sei.cmu.edu), a federally funded research and development center (FFRDC) operated by [Carnegie Mellon University](https://www.cmu.edu), is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks, accidents or failures.

- The Electronic Crimes Task Force of the [Secret Service](https://www.secretservice.gov) brings together federal, state and local law enforcement, prosecutors, private industry and academia to prevent, detect, mitigate and aggressively investigate attacks on the nation’s financial and critical infrastructures.

13. What is my responsibility for performing due diligence on third-party service providers?

Third-party service providers employed by a Member can pose various risks to the security of sensitive information and systems of the Member. Those risks can vary depending upon the nature of the relationship with the third party. Specifically, the third party could maintain access to a Member’s systems or sensitive information, provide data storage, and operate outsourced systems, among other services. A Member should utilize a risk-based approach to review how the third party is safeguarding the Member’s sensitive information and access to the Member’s systems, which may include asking questions of the third party or requesting additional supporting documentation.

14. What if a third-party service provider refuses to provide me with information necessary to make a determination on the ability of the third-party service provider to safeguard my information or access to my systems?

NFA recognizes that a Member’s ability to manage the security risks posed by third party service providers may be limited by the information these service providers elect to provide to the Member. Generally, a Member should perform due diligence on a critical service provider’s security practices and avoid using third parties whose security standards are not comparable to the Member’s standards in a particular area or activity. A Member should make its best effort to obtain enough information that it feels is relevant regarding the third party’s security standards, which could include discussions with other entities or individuals utilizing the same third party on their own satisfaction with the service provided. A Member could also consider adding security safeguard provisions to service-level agreements with third parties and should consider adopting procedures to place appropriate access controls to their information systems and data upon third-party service providers, and procedures to restrict or remove, on a timely basis, a third-party service provider’s access to their information systems once the service provider is no longer providing services.
15. Does NFA have a cybersecurity committee?
No. Relevant cybersecurity topics are discussed during NFA’s Compliance and Risk Committee, Executive Committee and Board of Director meetings, as applicable. NFA also maintains various Member-specific advisory committees where applicable cybersecurity topics may be discussed.

16. What defines a cybersecurity “breach”?
In general terms, a breach should include any unauthorized access to a Member’s sensitive information or systems by either intentional or unintentional means. Members should note, however, that many state and federal statutes define data breach in specific contexts.

17. When should I notify NFA, other regulatory agencies, or law enforcement of a cybersecurity breach?
Members should adopt a response plan within their ISSP that includes notification to NFA, relevant regulatory bodies and law enforcement based upon the type, severity, and materiality of an event and be familiar with notice requirements contained in applicable state and federal data breach statutes and regulations. Members are encouraged to obtain contact information for applicable regulatory bodies and law enforcement in advance of an event. Subsequent to an event, Members should also consider sharing the relevant details of a breach with a cybersecurity information-sharing network organization.

18. Must I train all employees on my ISSP?
The need to train employees, and the extent of such training, depends on the risks identified by the Member during its own risk assessment. Everyone employed by the Member must understand their responsibility for safeguarding personally identifiable information and the security of the Member’s systems. Of course, it may be appropriate to vary the level of training based on an employee’s access to particular systems and information.

19. What records must I maintain to evidence training provided to employees?
Records relating to employee training should include the topics covered (e.g. an agenda, presentation slides, etc.), a record of attendance (e.g. a sign-in sheet or learning management system log), and any other materials distributed as part of the training.

20. Will NFA coordinate with other regulators during exams and when responding to cybersecurity events?
NFA already endeavors to coordinate, where applicable, with other regulators on events impacting Members. NFA will continue its efforts to coordinate in order to make our examinations and responses to cybersecurity events as effective and efficient as possible.
21. Can NFA share best practices and other suggestions based on observations noted during exams?

Over time NFA will gain more knowledge of prudent cybersecurity practices at Member firms through examinations and meetings with other industry professionals and regulators. NFA intends to share additional guidance with Members as more experience with various cybersecurity practices are observed.

22. I am a non-US Swap Dealer operating under substituted compliance, must I comply with the Interpretation?

Yes. Non-US Swap Dealers have an obligation to comply with the Interpretive Notice’s requirements.

23. As a guarantor FCM, what is my responsibility for supervising my guaranteed introducing brokers’ (GIBs) compliance with the Interpretive Notice?

Compliance Rule 2-9 and corresponding Interpretive Notice 9019 impose a duty on guarantor FCMs to supervise the activities of their GIBs, which include day-to-day monitoring, on-site visits, and ongoing training. A Guarantor FCM should ensure that its GIBs have read and understand the Interpretive Notice, as well as, address in the FCM’s own security risk assessment the risks posed by its GIBs that have access to the FCM’s systems or sensitive information. To discharge their supervisory obligations, guarantor FCMs should also review annually with their GIBs the additional cybersecurity items added to NFA’s self-exam questionnaire to ensure the GIBs develop appropriate ISSPs for their business activities.

24. I missed NFA’s cybersecurity Member workshops. Are more planned?

No. While no additional workshops are planned, the audio recording and materials from NFA’s Chicago Cybersecurity Workshop are on NFA’s website. Members are encouraged to contact NFA with any additional questions. NFA intends to share additional guidance with Members as more experience with various cybersecurity practices are observed.

Contact NFA

If you have additional questions regarding NFA’s Interpretive Notice, please contact Dale Spoljaric, Managing Director, Compliance (dspoljaric@nfa.futures.org or 312-781-7415) or Shuna Awong, Director, OTC Derivatives (sawong@nfa.futures.org or 212-513-6057).