# The Practical Implications of the National Securities Clearing Corporation's New Cybersecurity Rules

**February 7, 2020**

Some increasingly familiar themes emerged from the U.S. Securities and Exchange Commission's ("SEC") quiet approval in December of a proposal amending the Rules and Procedures of the National Securities Clearing Corporation ("NSCC").[1] The new rules, which became effective immediately, require member entities and trade data organizations to periodically submit a "Cybersecurity Confirmation" to the NSCC representing that they have aligned their cybersecurity programs with industry standards. Such representations will be a condition for NSCC membership going forward. We discuss briefly here the practical takeaways of the new rules, but first the background.

## Who is covered?

To start, the new rules apply to:

- Existing NSCC members;
- Entities applying for membership, including those with pending applications; and
- Any entity that provides trade data to the NSCC for comparison and trade recording.

## When is the Confirmation required?

The rules became effective on December 9, 2019, immediately upon their adoption. Current members are required to provide their initial Cybersecurity Confirmation within 180 days of when the NSCC notifies the entity's pre-identified Control Officer.

---

[1] U.S. Securities and Exchange Commission, *Self-Regulatory Organizations; National Securities Clearing Corporation; Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program*, Release No. 34-87696, File No. SR-NSCC-2019-003 (Dec. 9, 2019), available here (pdf) [hereinafter "Order Approving Proposed Rule"].

Subsequent Cybersecurity Confirmations must then be submitted every two years. New applicants, including those with pending applications, must submit a Cybersecurity Confirmation as a part of the application process.

The new rules for trade data organizations are slightly different than those for current or future NSCC members. Because trade data organizations are not NSCC members, their relationship with the NSCC is governed by contract rather than the Rules and Procedures. Consequently, the new rules allow the NSCC to require a Cybersecurity Confirmation when determining whether to accept trade data from a non-member organization. The NSCC intended for this change to "provide transparency regarding the steps [the] NSCC may take when determining whether to accept trade data from such organizations."[2]

## What does the Confirmation require?

The new rules require that a "designated senior executive" attest to the cybersecurity matters contained in the Cybersecurity Confirmation provided to the NSCC.[3] The required disclosures will be set forth on a form provided by the NSCC, and will include representations relating to the following categories that are starting to look like what many regulators expect as part of a comprehensive cybersecurity program:

- *Governance*: The entity maintains a comprehensive risk-based cybersecurity program that considers potential cyber threats and protects the confidentiality, integrity, and availability of its systems and information.

- *Policies and Procedures*: The entity implemented and maintains a written enterprise cybersecurity policy that aligns with industry standards and is approved by senior management or the board. To satisfy this requirement, the company must identify the industry standard(s) to which it has aligned its practices. The NSCC identified a number of guidelines and standards as adequate for this purpose, including the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"), International Organization for Standards 27001/27002 ("ISO 27001"), and Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool.

- *Vendor Management:* The entity, if using a vendor to connect or manage the connection with the NSCC, has an appropriate program in place to evaluate the cyber risks and impact of such vendors and reviews third-party assurance reports.

---

2 Order Approving Proposed Rule, p. 9.

3 Order Approving Proposed Rule, p. 5.

- *Technical Safeguards*: The entity protects the segment of their system connecting to or interacting with the NSCC.

- *Incident Response Planning*: The entity established processes and procedures to identify and remediate cyber issues in compliance with applicable regulatory and/or statutory requirements.

- *Periodic Updates*: The entity reviews and updates its cybersecurity program periodically "based on a risk assessment or changes to technology, business, the threat ecosystem, and/or the regulatory environment."[4]

- *Review and Assessment*: The entity must represent that its cybersecurity program and framework has been reviewed against an industry standard framework, such as NIST CSF, ISO 27001, or the FFIEC Cybersecurity Assessment Tool. The following entities may conduct this review:

  - The company itself, if the company has filed a certification of Compliance with the Superintendent of the New York Department of Financial Services ("NYDFS");

  - A regulator;

  - An independent external entity with cybersecurity expertise; or

  - An internal independent audit function reporting directly to the company's board of directors.

## Don't I already have to do this?

In its proposal, the NSCC noted that many of its members may already be subject to one or more regulations requiring the implementation of a cybersecurity program, including, among others, Regulation S-P, Regulation S-ID, and the NYDFS Cybersecurity Regulation.[5] The NSCC further stated that it views compliance with the NYDFS Cybersecurity Regulation as sufficient to meet the objectives of the Cybersecurity Certification. Consequently, entities subject to NYDFS may be a step ahead of non-NYDFS regulated entities in complying with this reporting obligation, provided they can document that they have met the requirements underlying both compliance filings.

---

[4] Order Approving Proposed Rule, p. 6.

[5] Regulation S-P, 17 C.F.R. 248.1, *et seq.*; Regulation S-ID, 17 C.F.R 2483.201-2483.202; New York Department of Financial Services Cybersecurity Regulation, 21 NYCRR 500.

## Will the DTCC or NSCC review my cybersecurity program?

At least for the time being, the DTCC will sample a certain percentage of covered entities to test the accuracy of the representations made in the Cybersecurity Confirmation. These reviews will be conducted via WebEx, and will require entities to present their (1) cybersecurity program policies and procedures; (2) framework certification or proof of third-party assessment; and (3) other evidence relating to the Cybersecurity Confirmation.

## What are the practical implications?

Ultimately, the new rules present a handful of requirements and practical considerations that all member entities and trade data organizations should take into account when reviewing their cybersecurity program.

- To start, this is a new reporting requirement. Covered entities should mark their compliance calendars and determine which internal reviews and approvals must be completed before the Cybersecurity Confirmation can be filed, and also ensure that they have appointed a Control Officer for communications with the NSCC.

- The new rules also continue a trend by regulators of holding senior management (and boards) accountable for an entity's cybersecurity program. As with the NYDFS cyber certification, the entity and senior executive signing the Cybersecurity Confirmation will certainly want the protection of a well-documented program that clearly identifies the support for these new representations.

- The rules require alignment with one or more industry standard, risk-based frameworks, such as NIST CSF, FFIEC, or ISO 27001, among others. Covered entities should evaluate their cybersecurity programs to ensure that they incorporate the principles and standards reflected in at least one of these frameworks, and document the basis for security decisions regarding particular risks that may go against default expectations of regulators.

- Many covered entities are already using one or more of these frameworks to benchmark their cybersecurity programs. This is especially true for NYDFS-regulated entities, which likely leveraged one of these frameworks when conducting their required periodic risk assessment. Thoughtful planning to take advantage of the overlap with these types of existing requirements should avoid a lot of extra effort to assess and document compliance with the new rules.

- By tying the rules to risk-based industry frameworks, the NSCC is reaffirming the welcome view that cybersecurity is not "one size fits all." Each of the NSCC-recognized frameworks already incorporates this principle, and allows covered entities to apply the framework based upon the nature and character of the covered entity's business. While it is unlikely that regulators will second guess, within reason, choices made around particular cyber controls, they certainly will expect covered entities to have assessed the risks, thought about the range of choices, and made decisions they are prepared to explain.

- Similarly, the NSCC's use of industry standard frameworks, along with attestations to a specified list of cybersecurity program components, adds to the growing consensus of what constitutes a "reasonable cybersecurity program."

* * *

Please do not hesitate to contact us with any questions.

**NEW YORK**

Jeremy Feigelson
jfeigelson@debevoise.com

Avi Gesser
agesser@debevoise.com

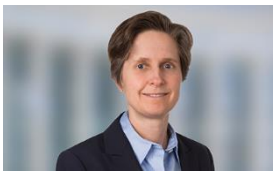
Jim Pastore
jjpastore@debevoise.com

Paul M. Rodel
pmrodel@debevoise.com

Lisa Zornberg
lzornberg@debevoise.com

## WASHINGTON, D.C.


Luke Dembosky
ldembosky@debevoise.com


Julie M. Riewe
jriewe@debevoise.com


H Jacqueline Brehmer
hjbrehme@debevoise.com


Taryn Elliott
taelliot@debevoise.com