CYBERSECURITY
Checklist for a Small Firm's Cybersecurity Program

Firm Name:	
Person(s) Responsible for Cybersecurity Program:	
Last Updated:	
Key Personnel:	

Last Updated: (FINRA's last update)	Version 1.1 December 2016

Important:

Cybersecurity is broadly defined as the protection of investor and firm information from compromise through the use—in whole or in part—of information technology. Compromise refers to a loss of data confidentiality, integrity or availability. This checklist is provided to assist small member firms with limited resources to establish a cybersecurity program to identify and assess cybersecurity threats, protect assets from cyber intrusions, detect when their systems and assets have been compromised, plan for the response when a compromise occurs and implement a plan to recover lost, stolen or unavailable assets. This checklist is primarily derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and FINRA's Report on Cybersecurity Practices. Please consult the NIST framework and FINRA's Report for a more in-depth discussion on the subjects listed herein.

National Institute of Standards and Technology (NIST) Cybersecurity Framework
SANS Critical Security Controls for Effective Cyber Defense
FINRA's Report on Cybersecurity Practices

Legend for Text Entry Fields

	Enter Free Text
	Pre-Populated Fields
	Choose from Drop Down List
	Locked Down Fields
	Insert Rows

Using this checklist is optional:

This checklist is not exhaustive and firms should address their cybersecurity program in a way that best suits their business model. There is no one-size-fits-all cybersecurity program. Firms may choose to develop or use their own checklist, borrow sections from this checklist to include in their own checklist, or use a different resource (e.g., SIFMA's small firm check list, NIST guidance, or the Securities and Exchange Commission's guidance). Firms that use this checklist must adapt it to reflect their particular business, products, and customer base. Use of this checklist does not create a "safe harbor" with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements.

Methodology:

Using this checklist, firms will identify and inventory their digital assets, assess the adverse impact to customers and the firm if the assets were compromised, identify potential protections and processes that secure the assets, and then make a risk-based assessment considering their resources, the consequences of a potential breach and available protections and safeguards. Firms may decide to remediate or address some high level risk impact vulnerabilities or they may decide that the threat is a low level risk impact which they can accept. Firms should articulate why they decided to remediate or chose not to remediate. Completing this checklist will require time and effort from senior executives at the firm. At a minimum, firms should know the assets that are vulnerable to a cyber-incident, and they should assign a risk level to these assets. Senior executives will then be informed on how best to allocate firm resources to protect the firm's and customers' information. **See below for questions.**

Assistance:

At small firms, one person may be responsible for operations, compliance and legal functions including the cybersecurity program, and he or she may not understand the technology at issue or terms used in this checklist. In this instance, the firm may consider working with outside technology help, industry trade associations or other peer groups, their vendors or their FINRA Regulatory Coordinator to understand the information discussed in this checklist. Many small firms rely on clearing firms and vendors to maintain customer accounts and transact business but these small firms should not assume that others are responsible for preventing or reacting to a cyber-incident.

Using Excel:

This checklist is in Excel and uses Excel formulas. The person completing this checklist should have a basic knowledge of Excel. If no one at the firm has these skills, please send an email to **memberrelations@finra.org** to schedule a call. There are also many helpful video tutorials on Excel available on YouTube.

Please note: If you need to insert a new row in Section 1, you will also need to insert rows on the other Sections and copy the pre-existing formulas into the newly inserted cells.

CYBERSECURITY
Checklist for a Small Firm's Cybersecurity Program

Firm Name:	
Person(s) Responsible for Cybersecurity Program:	
Last Updated:	
Key Personnel:	

Checklist Methodology
Please review the five questions below and based upon your answers, you should complete the sections (12 tabs total) applicable to your business. The five core sections of the checklist follow the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.
Questions about your firm's assets and systems:

1) Do you store, use or transmit personally identifiable information (PII) (e.g., social security numbers or date of birth) or firm sensitive information (e.g. financial records) electronically?
If you answer yes to question 1, you will fill out the following sections of the Cybersecurity Checklist:
Section 1 - Identify and Assess Risks: Inventory
Section 2 - Identify and Assess Risks: Minimize Use
Section 4 - Protect: Information Assets
Section 6 - Protect: Encryption
Section 8 - Protect: Controls and Staff Training
Section 9 - Detect: Penetration Testing
Section 10 - Detect: Intrusion
Section 11 - Response Plan

2) Do you transmit PII or firm sensitive information to a third party, or otherwise allow access to your PII or firm sensitive information by a third party?
If you answer yes to question 2, you will fill out:
Section 3 - Identify and Assess Risks: Third Party Access

3) Do your employees (or independent contractors) maintain devices that access PII or firm sensitive information?
If you answer yes to question 3, you will fill out:
Section 7 - Protect: Employee Devices

4) Do you have assets that if lost or made inoperable would impact your firm's operations (e.g., trading or order management systems)?
If you answer yes to question 4, you will fill out:
Section 5 - Protect: Systems Assets

5) If your systems, PII or firm sensitive information were made inoperable or stolen, would you need to recover them to conduct business?
If you answer yes to question 5, you will fill out:
Section 12 - Recovery