# REQUEST FOR PUBLIC COMMENT REGARDING A PROPOSED INVESTMENT ADVISER MODEL RULE FOR INFORMATION SECURITY AND PRIVACY UNDER THE UNIFORM SECURITIES ACTS OF 1956 AND 2002[1]

**September 23, 2018**

The North American Securities Administrators Association, Inc. ("NASAA") is requesting public comment on a proposed investment adviser model rule to address information security and privacy, a proposed amendment to the investment adviser NASAA model Recordkeeping Requirements rule, and a proposed amendment to the NASAA model Unethical Business Practices of Investment Advisers, Investment Adviser Representatives, and Federal Covered Advisers rule (collectively, "Rule Proposal").

The Rule Proposal has three components. First, a proposed model rule to require investment advisers to adopt policies and procedures regarding information security (both physical security and cybersecurity) and to deliver its privacy policy annually to clients ("Proposed Information Security and Privacy Rule"). Second, a proposed amendment to the existing investment adviser NASAA model recordkeeping requirements rule to require that investment advisers maintain these records ("Proposed Recordkeeping Rule Amendment"). Finally, a proposed amendment to the existing investment adviser NASAA model Unethical Business Practices of Investment Advisers, Investment Adviser Representatives, and Federal Covered Advisers and the Prohibited Conduct in Providing Investment Advice model rules (collectively "UBP Model Rules") to include failing to establish, maintain, and enforce a required policy or procedure to the enumerated list of unethical business practices/prohibited conduct ("Proposed Unethical Business Practices Rules Amendment").

Comments on the Rule Proposal are due on or before **November 26, 2018**. To facilitate consideration of comments, please send comments to Andrea Seidt (Andrea.Seidt@com.state.oh.us), Investment Adviser Section Chair; Elizabeth Smith (Elizabeth.Smith@dfi.wa.gov), Investment Adviser Regulatory Policy and Review Project Group Chair; and the NASAA Legal Department (nasaacomments@nasaa.org).

We encourage, but do not require, comments to be submitted by e-mail. Hard copy comments can be submitted at the address below.

NASAA Legal Department
750 First Street, NE, Suite 1140
Washington, DC 20002

***Note:*** *After the comment period has closed, NASAA will post to its website the comments it receives as submitted by the authors. Parties should therefore only submit information that they wish to make publicly available. Further, the following notice will appear on NASAA's website where comments are*

[1] This proposal also includes related amendments to the NASAA model Recordkeeping Requirements rule and the NASAA model Unethical Business Practices rule.

*posted: NASAA, its agents, and employees accept no responsibility for the content of the comments posted on this Web page. The views, expressions, and opinions expressed in the comments are solely those of the author(s) of the comments.*

## Rule Proposal

## I. Background

NASAA has been actively working on the various investment adviser-related needs and concerns regarding cybersecurity for multiple years. The focus has been on protecting and educating both investment advisers and the investing public. The NASAA Investment Adviser Section researched the existing cybersecurity frameworks and protocols, the potential for investor harm, and the need for additional guidance and support among the state-registered investment adviser population.

NASAA identified a significant need for more information and tools regarding cybersecurity. In 2014, NASAA published a compilation of results of a pilot survey of cybersecurity practices of small and mid-sized investment adviser firms. The results showed that investment advisers were utilizing multiple types of technology to support their businesses and that investment advisers themselves wanted more guidance on how to better secure confidential information in their operations.[2]

Due to these results, the NASAA Investment Adviser Section tasked multiple project groups within the Investment Adviser Section to work together to holistically address the cybersecurity needs within the state-registered investment adviser community. This work resulted in three important NASAA initiatives to date, described below:

1. Examinations – NASAA Project Groups developed cybersecurity questions for examiners and added these questions into NASAA's 2017 coordinated investment adviser examination reporting. The results were compelling. A series of more than 1,200 coordinated examinations of state-registered investment advisers by state securities examiners in a six-month period uncovered 590 cybersecurity deficiencies.[3]

2. Education - NASAA rolled out a Cybersecurity Checklist in 2017 to help state-registered investment advisers evaluate their cybersecurity risks and to provide direct guidance on ways the firms can identify, respond, and recover from cybersecurity weaknesses and/or breaches. NASAA is currently working on additional tools and an instructional webinar on how investment advisers can make best use of the checklist. This Rule Proposal directly complements NASAA's cybersecurity tools and educational efforts.

3. Regulatory/Model Rulemaking – NASAA model rule to require investment advisers to adopt policies and procedures regarding information security. This dual approach is based on the understanding that most investment advisers know the importance of information security

[2] Available at http://www.nasaa.org/industry-resources/investment-advisers/nasaa-cybersecurity-report/.
[3] Available at http://www.nasaa.org/43287/state-investment-adviser-examinations-uncover-cybersecurity-deficiencies/.

measures and want some assistance in these areas but are reluctant or neglectful in adopting appropriate policies, procedures, and practices until they are given the necessary tools, guidance, and directive to do so.

This Rule Proposal represents the third effort listed above.

While states can independently require investment advisers to adopt information security policies and procedures through existing state statutes or rules, NASAA hopes the Rule Proposal accomplishes the following three objectives:

(1) Highlight the importance of data privacy and security in our financial markets along with the concomitant need for investment advisers to have information security policies and procedures;

(2) Provide a basic structure for how state-registered investment advisers may design their information security policies and procedures; and

(3) Create uniformity in both state regulation and state-registered investment adviser practices.

## II. Overview of the Rule Proposal

The Proposed Information Security and Privacy Rule and the Proposed Recordkeeping Rule Amendment are drafted pursuant to the Post-Registration Provisions and Requirements contained in Section 203 of the Uniform Securities Act of 1956 and Section 411 of the Uniform Securities Act of 2002. We note that upholding such obligations is also inherent to an investment adviser's fiduciary duty, pursuant to Section 102 of the Uniform Securities Act of 1956 and Section 502 of the Uniform Securities Act of 2002. The Proposed Unethical Business Practices Rules Amendment is written pursuant to Section 102 of the Uniform Securities Act of 1956 and Section 502 of the Uniform Securities Act of 2002.

While proper information security is inherent to an investment adviser's fiduciary duty, a NASAA model rule regarding information security could be written pursuant to the post-registration provisions and requirements or the anti-fraud prohibitions contained within the Uniform Acts. The Securities and Exchange Commission ("SEC") enacted many of its policies and procedures pursuant to Section 206(4) of the Investment Advisers Act (Prohibited Transactions by Investment Advisers)[4] and then created specific corresponding recordkeeping requirements for those rules. However, the Rule Proposal uses the Post-Registration Provisions and Requirements as the statutory authority for the Proposed Information Security and Privacy Rule, rather than the anti-fraud provisions of the Uniform Acts. This decision is based on a number of factors, including consistency with most of the existing NASAA model rules regarding policies and procedures.

[4] *See* 15 U.S.C. § 80b-6(4)

Information security is complex and, in general, rules-based. Information security is an area where compliance-oriented regulations may provide the best outcomes for both investment advisers and the investing public. However, investment adviser regulations are, in general, principles-based. The Proposed Information Security and Privacy Rule is designed to maintain a principles-based philosophy while containing some compliance-oriented features. This keeps the proposed rule consistent with the general principles-based investment adviser regulations while recognizing that more specifics regarding information security may be necessary to protect the investing public and also helpful to investment advisers requesting clearer guidance.

The Rule Proposal has three parts: (1) the Proposed Information Security and Privacy Rule; (2) the related Proposed Recordkeeping Rule Amendment; and (3) the related Proposed Unethical Business Practices (UBP) Rules Amendment.

### *1. Proposed Information Security and Privacy Rule*

The Proposed Information Security and Privacy Rule is divided into two parts: (a) Physical Security and Cybersecurity Policies and Procedures, and (b) Privacy Policy.

#### *a) Physical Security and Cybersecurity Policies and Procedures*

The Physical Security and Cybersecurity Policies and Procedures section contains the requirement that investment advisers adopt policies and procedures regarding information security. This section is based on existing and widely used information security concepts, rules, and frameworks. It is not intended to create a new cybersecurity protocol.

The Physical Security and Cybersecurity Policies and Procedures section contains the Header to this section of the rule, Subsection (1), Subsection (2), and Subsection (3). The Physical Security and Cybersecurity Policies and Procedures Header states:

> ***Physical Security and Cybersecurity Policies and Procedures.*** *Every investment adviser shall establish, implement, update, and enforce written physical security and cybersecurity policies and procedures reasonably designed to ensure the confidentiality, integrity, and availability of physical and electronic records and information. The policies and procedures must be tailored to the investment adviser's business model, taking into account the size of the firm, type(s) of services provided, and the number of locations of the investment adviser.*

The Header to the section introduces the written physical security and cybersecurity policies and procedures requirement. The requirement is structured using the CIA Triad: Confidentiality, Integrity, and Availability. The CIA Triad is a widely used and well-known model for security policy development.[5] Exhibit B to this public comment proposal contains more information about the CIA Triad.

[5] Exhibit B to this Rule Proposal contains more information about the CIA Triad

Furthermore, the Header specifies that the policies and procedures must be reasonably designed. Finally, the Header specifies that the policies and procedures must take into account the investment adviser's business model. This is the same principle behind the design of the NASAA Model Rule on Business Continuity and Succession Planning.[6]

### *(a)(1) Subsection (a)(1) of the Physical Security and Cybersecurity Policies and Procedures Rule*

**(1)** The physical security and cybersecurity policies and procedures must:

**(A)** Protect against reasonably anticipated threats or hazards to the security or integrity of client records and information;

**(B)** Ensure that the investment adviser safeguards confidential client records and information; and

**(C)** Protect any records and information the release of which could result in harm or inconvenience to any client.

This first subsection of the Physical Security and Cybersecurity Policies and Procedures rule is based on the Gramm-Leach-Bliley Act's protection of non-public personal information provision[7], the Federal Trade Commission's ("FTC") Safeguard Rules: Standards for Safeguarding Customer Information[8], and the Securities and Exchange Commission's ("SEC") rule regarding procedures to safeguard customer records and information.[9]

This section is written to best serve the needs of state-registered investment advisers and the investing public. As many of the FTC's Safeguard Rules apply to state-registered investment advisers, the Proposed Information Security and Privacy Rule was written to be compatible with those rules.

### *(a)(2) Subsection (a)(2) of the Physical Security and Cybersecurity Policies and Procedures Rule*

**(2)** The physical security and cybersecurity policies and procedures must cover at least five functions:

**(A)** Identify. Develop the organizational understanding to manage information security risk to systems, assets, data, and capabilities;

**(B)** Protect. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;

---

[6] *See* North American Securities Administrators Association, Inc., (April 13, 2015), *NASAA Model Rule on Business Continuity and Succession Planning Model Rule 203(a)-1A or 2002 Rule 411(c)-1A, available at* http://www.nasaa.org/wp-content/uploads/2011/07/NASAA-Model-Rule-on-Business-Continuity-and-Succession-Planning-with-gu....pdf
[7] *See* 15 U.S.C § 6801
[8] *See* 16 CFR § 314.3
[9] *See* 17 CFR 248.30(a). Rule 30 of Regulation S-P

**(C)** Detect. Develop and implement the appropriate activities to identify the occurrence of an information security event;

**(D)** Respond. Develop and implement the appropriate activities to take action regarding a detected information security event; and

**(E)** Recover. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an information security event.

This second subsection of the rule ties the National Institute of Standards and Technology ("NIST") Framework's five Functions into the Proposed Information Security and Privacy Rule.[10] NIST is a federal agency within the Unites States Department of Commerce. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve quality of life.

The NIST Cybersecurity Framework was developed in response to Presidential Executive Order 13636[11], "Improving Critical Infrastructure Security." After the Cybersecurity Enhancement Act of 2014[12], NIST was tasked with the development of voluntary, industry-led cybersecurity standards and best practices. NIST has developed a widely used voluntary Framework that consists of standards, guidelines, and best practices to help organizations manage their cybersecurity risk.

The core of the NIST Framework consists of five Functions: Identify, Protect, Detect, Respond, and Recover. The language for this subsection is directly quoted from the United States Computer Emergency Readiness Team's website, which includes the NIST Framework's five Functions.[13] The Rule Proposal mirrors this language in an attempt to clarify that the rule does not create a new framework or new functions.[14] Exhibit B to this public comment proposal contains more information about the NIST Functions.

By using the NIST Framework, the Rule Proposal, in conjunction with the NASAA Cybersecurity Checklist, is designed to help investment advisers better understand how they can identify, protect, detect, and respond to cyber incidents, as well as recover from a cybersecurity event. The NASAA Checklist is a living document designed to evolve and adapt to technological advances. The Rule Proposal and the NASAA Checklist are designed to encourage investment advisers to ask questions about their own cybersecurity posture: what are they currently doing, where they are most vulnerable, and how they could do things better.

---

[10] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (April 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[11] Exec. Order No. 13636, 3 C.F.R. 13636 (2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
[12] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274 (2014)
[13] https://www.us-cert.gov/ccubedvp/cybersecurity-framework.
[14] Exhibit B to this Rule Proposal contains more information about the NIST Functions

***(a)(3) Subsection (a)(3) of the Physical Security and Cybersecurity Policies and Procedures Rule***

> **(3) Maintenance.** The investment adviser must review, no less frequently than annually, and modify, as needed, these policies and procedures to ensure the adequacy of the security measures and the effectiveness of their implementation.

This final subsection covers the investment adviser's maintenance requirements. The rule requires that the investment adviser test both the adequacy and the effectiveness of the policies and procedures. Furthermore, it requires that the investment adviser update the policies and procedures. This is in addition to the requirement that investment advisers keep the policies and procedures "current" as will be required in the recordkeeping rule.

***b) Privacy Policy***

> **Privacy Policy.** The investment adviser must deliver upon the investment adviser's engagement by a client, and on an annual basis thereafter, a privacy policy to each client that is reasonably designed to aid in the client's understanding of how the investment adviser collects and shares, to the extent permitted by state and federal law, non-public personal information. The investment adviser must promptly update and deliver to each client an amended privacy policy if any of the information in the policy becomes inaccurate.

The Proposed Information Security and Privacy Rule's second section is regarding the investment adviser's privacy policy. As state-registered investment advisers are required by the FTC to maintain and deliver a privacy policy to their clients, the Privacy Policy section is included in the Rule Proposal but separated from the Physical Security and Cybersecurity Policies and Procedures Rule.

The FTC's rule does not currently automatically require annual delivery. The Proposed Information Security and Privacy Rule is not written to create a new privacy policy requirement. However, the Proposed Information Security and Privacy Rule requires annual delivery of the privacy policy.

Privacy policies contain important information, and advisory clients should receive a copy of their investment adviser's privacy policy every year. It is important to note that while the Proposed Rule requires that the investment adviser deliver its privacy policy annually to clients, the Rule Proposal does not require the investment adviser deliver a copy of its Physical Security and Cybersecurity Policies and Procedures to clients.

***2. Proposed Recordkeeping Rule Amendment***

The second part of the Rule Proposal is an amendment to the existing investment adviser NASAA Recordkeeping Requirements For Investment Advisers Model Rule 203(a)-2[15] to require that investment

[15] *See* North American Securities Administrators Association, Inc., (Adopted 9/3/1987 and subsequently amended), *Recordkeeping Requirements For Investment Advisers Model Rule 203(a)-2, available at* http://www.nasaa.org/wp-content/uploads/2011/07/IA-Model-Rule-Recordkeeping.pdf

advisers maintain records relating to the Proposed Information Security and Privacy Rule. The Proposed Recordkeeping Rule Amendment provides amendments to both alternatives contained in the Model Recordkeeping Requirements Rule. This amendment requires that the investment adviser maintain the policies and procedures, records documenting compliance, and records of any violations. Additionally, the Proposed Recordkeeping Rule Amendment specifically requires that the investment adviser maintain a hard copy of the current policies and procedures in a separate location. While the NASAA Model Recordkeeping Requirements rule permits electronic storage, given the nature of information security risks, investment advisers should maintain a hard copy of these policies and procedures in a separate location.

### *3. Proposed Unethical Business Practices (UBP) Amendment*

The final part of the Rule Proposal is an amendment to the existing investment adviser NASAA Model Unethical Business Practices of Investment Advisers, Investment Adviser Representatives, and Federal Covered Advisers Model Rule 102(a)(4)(1) and the Prohibited Conduct of Investment Advisers, Investment Adviser Representatives and Federal Covered Investment Advisers Model Rule USA 2002 502(b) to include that failing to establish, maintain, and enforce a required policy or procedure would be an unethical business practice/prohibited conduct. This amendment is intended to cover all required policies and procedures, including, but not limited to, supervision and business continuity and succession in addition to the Proposed Information Security and Privacy Rule. State and federal laws impose various requirements regarding policies and procedures on state-registered investment advisers.

## III. Request for Comment

NASAA requests public comment on the Rule Proposal. In particular:

(1) Do you support the Rule Proposal?

(2) Do you recommend changes to the Proposed Information Security and Privacy Rule?

   a. Physical Security and Cybersecurity Policies and Procedures:
      i. Are there additional information security areas the Rule should cover?

   b. Privacy Policy:
      i. Do you support the annual delivery requirement?

(3) Do you recommend changes to the Proposed Recordkeeping Rule Amendment?

(4) Do you recommend changes to the Proposed Unethical Business Practices (UBP) Amendment?

(5) Do you anticipate any specific obstacles to implementation of the Rule Proposal by state registered investment advisers?

(6) Are there any additional areas for investment adviser information security education or tools that you would like NASAA to provide, including, but not limited to, solutions to perceived obstacles to implementation by state registered investment advisers?

## IV. Conclusion

Comments on the Rule Proposal are due by **November 26, 2018**. The following documents are attached to this Rule Proposal:

- Rule Proposal – *Exhibit A*
- Information Security Frameworks and Measures – *Exhibit B*
- NASAA Cybersecurity Checklist – *Exhibit C*

# Exhibit A

**Rule Proposal**

## I. Proposed Information Security and Privacy Rule

**Investment Adviser Information Security and Privacy Rule [NEW 1956 & 2002 MODEL ACT RULE NUMBERS]**

(a) **Physical Security and Cybersecurity Policies and Procedures.** Every investment adviser shall establish, implement, update, and enforce written physical security and cybersecurity policies and procedures reasonably designed to ensure the confidentiality, integrity, and availability of physical and electronic records and information. The policies and procedures must be tailored to the investment adviser's business model, taking into account the size of the firm, type(s) of services provided, and the number of locations of the investment adviser.

(1) The physical security and cybersecurity policies and procedures must:

(A) Protect against reasonably anticipated threats or hazards to the security or integrity of client records and information;

(B) Ensure that the investment adviser safeguards confidential client records and information; and

(C) Protect any records and information the release of which could result in harm or inconvenience to any client.

(2) The physical security and cybersecurity policies and procedures must cover at least five functions:

(A) Identify. Develop the organizational understanding to manage information security risk to systems, assets, data, and capabilities;

(B) Protect. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;

(C) Detect. Develop and implement the appropriate activities to identify the occurrence of an information security event;

(D) Respond. Develop and implement the appropriate activities to take action regarding a detected information security event; and

(E) Recover. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an information security event.

(3) **Maintenance.** The investment adviser must review, no less frequently than annually, and modify, as needed, these policies and procedures to ensure the adequacy of the security measures and the effectiveness of their implementation.

(b) **Privacy Policy.** The investment adviser must deliver upon the investment adviser's engagement by a client, and on an annual basis thereafter, a privacy policy to each client that is reasonably designed to aid in the client's understanding of how the investment adviser collects and shares, to the extent permitted by state and federal law, non-public personal information. The investment adviser must promptly update and deliver to each client an amended privacy policy if any of the information in the policy becomes inaccurate.

## II. Proposed Recordkeeping Rule Amendment

### NASAA Recordkeeping Requirements For Investment Advisers Model Rule

Rule 203(a)-2 or Rule USA 2002 411(c)-1 Recordkeeping Requirements [ALTERNATIVE 1]:

(a) Every investment adviser registered or required to be registered under the Act shall make and keep true, accurate and current the following books, ledgers and records:

. . .

24.

(i) A copy of the investment adviser's Physical Security and Cybersecurity Policies and Procedures and Privacy Policy pursuant to [INSERT RULE CITATION]. In addition to the investment adviser's recordkeeping requirements pursuant to sections (e) and (g) of this rule, the investment adviser must maintain a current copy of these policies and procedures in hard copy in a separate location;

(ii) All records documenting the investment adviser's compliance with [INSERT RULE CITATION], including, but not limited to, evidence of the annual review of the policies and procedures;

(iii) A record of any violation of the [INSERT RULE CITATION], and of any action taken as a result of the violation.

Rule 203(a)-2 or Rule USA 2002 411(c)1 Recordkeeping Requirements [ALTERNATIVE 2] (Language for states which incorporate by reference Rule 204-2 of the Investment Advisers Act of 1940):

(a) Every investment adviser registered or required to be registered under this Act shall make and keep true; accurate and current the following books, ledgers and records:

. . .

14.

(i) A copy of the investment adviser's Physical Security and Cybersecurity Policies and Procedures and Privacy Policy pursuant to [INSERT RULE CITATION]. In addition to the investment adviser's recordkeeping requirements pursuant to sections (b) of this rule, the investment adviser must maintain a current copy of these policies and procedures in hard copy in a separate location;

(ii) All records documenting the investment adviser's compliance with [INSERT RULE CITATION], including, but not limited to, evidence of the annual review of the policies and procedures;

(iii) A record of any violation of the [INSERT RULE CITATION], and of any action taken as a result of the violation.

## III. Proposed Unethical Business Practices Model Rules Amendment

### NASAA Unethical Business Practices Of Investment Advisers, Investment Adviser Representatives, And Federal Covered Advisers Model Rule 102(a)(4)-1

Rule 102(a)(4)-1 Unethical Business Practices Of Investment Advisers, Investment Adviser Representatives, And Federal Covered Advisers

*[Introduction] A person who is an investment adviser, an investment adviser representative or a federal covered adviser is a fiduciary and has a duty to act primarily for the benefit of its clients. The provisions of this subsection apply to federal covered advisers to the extent that the conduct alleged is fraudulent, deceptive, or as otherwise permitted by the National Securities Markets Improvement Act of 1996 (Pub. L. No. 104-290). While the extent and nature of this duty varies according to the nature of the relationship between an investment adviser or an investment adviser representative and its clients and the circumstances of each case, an investment adviser, an investment adviser representative or a federal covered adviser shall not engage in unethical business practices, including the following:*

. . .

(w) Failing to establish, maintain, and enforce a required policy or procedure.

### NASAA Prohibited Conduct of Investment Advisers, Investment Adviser Representatives and Federal Covered Investment Advisers Model Rule USA 2002 502(b)

Rule USA 2002 502(b) Prohibited Conduct in Providing Investment Advice

*A person who is an investment adviser, an investment adviser representative or a federal covered investment adviser is a fiduciary and has a duty to act primarily for the benefit of its clients. The provisions of this subsection apply to federal covered investment advisers to the extent that the conduct alleged is fraudulent, deceptive, or as otherwise permitted by the National Securities Markets Improvement Act of 1996. While the extent and nature of this duty varies according to the nature of the relationship between an investment adviser, an investment adviser representative or a federal covered investment adviser and its clients and the circumstances of each case, an investment adviser, an investment adviser representative or a federal covered investment adviser shall not engage in prohibited fraudulent, deceptive, or manipulative conduct, including but not limited to the following:*

. . .

(w) Failing to establish, maintain, and enforce a required policy or procedure.

# Exhibit B

## Information Security Frameworks and Measures

After researching the existing frameworks and protocols, the NASAA Investment Adviser Section determined that any NASAA investment adviser information security initiative projects should follow the existing CIA Triad and NIST Framework. These concepts are widely used as building blocks to information security policies and procedures.

*CIA Triad*[16]

The CIA Triad is a widely used and well-known model for security policy development. Most information security measures should address how to protect the confidentiality of data, preserve the integrity of data, and promote the availability of data for authorized uses. These three concepts – Confidentiality, Integrity, and Availability – form the CIA Triad. All three of these are critical in information security policies and procedures.

Confidentiality is general information privacy. Confidentiality measures are designed to make sure that data is restricted to only the authorized people who need access to the specific data. Confidentiality measures should prevent sensitive information from reaching unauthorized persons and are designed to prevent a breach. The measures vary widely, typically based on amount and type of damage that could be done should the data fall into unintended hands.

Integrity is the goal of keeping data accurate and trustworthy by protecting data from intentional or accidental changes. Integrity measures can include three goals: (1) prevent unauthorized users from making modifications to data or programs; (2) prevent authorized users from making improper or unauthorized modifications; and (3) maintain internal and external consistency of data and programs.

Availability is intended to address the reliable access to the information by authorized people. Availability measures are intended to keep data and resources available for authorized use, especially during emergencies or disasters. Availability measures are typically structured to address common challenges, including: (1) normal equipment failures; (2) denial of service because of undiscovered flaws in implementation or intentional attacks; (2) loss of information and system capabilities because of natural disasters or human actions.

*NIST Framework*[17]

The National Institute of Standards and Technology (NIST) is a federal agency within the Unites States Department of Commerce. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST is also responsible for establishing information security standards and guidelines for federal agencies. Many

[16] The CIA Triad is sometimes referred to as the AIC Triad.
[17] https://www.nist.gov/cyberframework/framework

private sector organizations also use these standards and guidelines. According to the NIST website, the NIST Framework is “voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.”

The core of the NIST Framework consists of five Functions: Identify, Protect, Detect, Respond, and Recover. While the NIST Framework is complex, these five concurrent and continuous Functions can provide a relatively straightforward guide to help an organization manage its information security risks. While there is not a guaranteed way to protect an organization from information security risk, the Functions should help organizations minimizing damage and impact.

The United States Computer Emergency Readiness Team succinctly explains the five NIST Functions:

> **Identify:** Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
>
> **Protect:** Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.
>
> **Detect:** Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
>
> **Respond:** Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

**Recover:** Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.[18]

[18] https://www.us-cert.gov/ccubedvp/cybersecurity-framework

# Exhibit C

**NASAA Cybersecurity Checklist**

In 2017, NASAA published a Cybersecurity Checklist for state-registered investment advisers. The Cybersecurity Checklist is intended to be adaptive. It is structured into five parts based on the NIST Framework's five Functions: Identify, Protect, Detect, Respond, and Recover. The Checklist currently has nine items under Identify to consider. The Protect section is divided into six subsections: Use of Electronic Mail, Devices, Use of Cloud Services, Use of Firm Websites, Custodians & Other Third-Party Vendors, and Encryption. The Detect section covers anti-virus and firewalls. The Respond section has four items to consider to plan for how to respond to a cyber-event. The Recover section focuses on both cyber-insurance and disaster recovery. *See next page.*

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

# Cybersecurity Checklist for Investment Advisers

Identify | Protect | Detect | Respond | Recover

| Identify: Risk Assessments & Management | YES | NO | N/A |
|---|---|---|---|
| 1. Risk assessments are conducted frequently (e.g. annually, quarterly). | | | |
| 2. Cybersecurity is included in the risk assessment. | | | |
| 3. The risk assessment includes a review of the data collected or created, where the data is stored, and if the data is encrypted. | | | |
| 4. Internal "insider" risk (e.g. disgruntled employees) and external risks are included in the risk assessment. | | | |
| 5. The risk assessment includes relationships with third parties. | | | |
| 6. Adequate policies and procedures demonstrate expectations of employees regarding cybersecurity practices (e.g. frequent password changes, locking of devices, reporting of lost or stolen devices, etc.). | | | |
| 7. Primary and secondary person(s) are assigned as the central point of contact in the event of a cybersecurity incident. | | | |
| 8. Specific roles and responsibilities are tasked to the primary and secondary person(s) regarding a cybersecurity incident. | | | |
| 9. The firm has an inventory of all hardware and software. | | | |
| **Protect: Use of Electronic Mail** | YES | NO | N/A |
| 1. Identifiable information of a client is transmitted via email. | | | |
| 2. Authentication practices for access to email on all devices (computer and mobile devices) is required. | | | |
| 3. Passwords for access to email are changed frequently (e.g. monthly, quarterly). | | | |
| 4. Policies and procedures detail how to authenticate client instructions received via email. | | | |

| | | | |
|---|---|---|---|
| 5. Email communications are secured. (If the response is no, proceed to the next question.) | | | |
| 6. Employees and clients are aware that email communication is not secured. | | | |
| **Protect: Devices** | YES | NO | N/A |
| 1. Device access (physical and digital) is permitted for authorized users, including personnel and clients. | | | |
| 2. Device access is routinely audited and updated appropriately. | | | |
| 3. Devices are routinely backed up and underlying data is stored in a separate location (i.e. on an external drive, in the cloud, etc.) | | | |
| 4. Backups are routinely tested. | | | |
| 5. The investment adviser has written policies and procedures regarding destruction of electronic data and physical documents. | | | |
| 6. Destruction of electronic data and physical documents are destroyed in accordance with written policies and procedures. | | | |
| **Protect: Use of Cloud Services** | YES | NO | N/A |
| 1. Due diligence has been conducted on the cloud service provider prior to signing an agreement or contract. | | | |
| 2. As part of the due diligence, the investment adviser has evaluated whether the cloud service provider has safeguards against breaches and a documented process in the event of breaches. | | | |
| 3. The investment adviser has a business relationship with the cloud service provider and has the contact information for that entity. | | | |
| 4. The investment adviser is aware of the assignability terms of the contract. | | | |
| 5. The investment adviser understands how the firm's data is segregated from other entities' data within the cloud service. | | | |
| 6. The investment adviser is familiar with the restoration procedures in the event of a breach or loss of data stored through the cloud service. | | | |
| 7. The investment adviser has written policies and procedures in the event that the cloud service provider is purchased, closed, or otherwise unable to be accessed. | | | |

| | | | |
|---|---|---|---|
| 8. The investment adviser solely relies on free cloud storage. | | | |
| 9. The investment adviser has a back-up of all records off-site. | | | |
| 10. Data containing sensitive or personally identifiable information is stored through a cloud service. | | | |
| 11. Data containing sensitive or personally identifiable information, which is stored through a cloud service, is encrypted. | | | |
| 12. The investment adviser has written policies and procedures related to the use of mobile devices by staff who access data in the cloud. | | | |
| 13. The cloud service provider (or its staff) may access and/or view the investment adviser's data stored in the cloud. | | | |
| 14. The investment adviser allows remote access to its network (e.g. through use of VPN). | | | |
| 15. The VPN access of employees is monitored. | | | |
| 16. The investment adviser has written policies and procedures related to the termination of VPN access when an employee resigns or is terminated. | | | |
| **Protect: Use of Firm Websites** | YES | NO | N/A |
| 1. The investment adviser relies on a parent or affiliated company for the construction and maintenance of the website. | | | |
| 2. The investment adviser relies on internal personnel for the construction and maintenance of the website. | | | |
| 3. The investment adviser relies on a third-party vendor for the construction and maintenance of the website. | | | |
| 4. If the investment adviser relies on a third party for website maintenance, there is an agreement with the third party regarding the services and the confidentiality of information. | | | |
| 5. The investment adviser can directly make changes to the website. | | | |
| 6. The investment adviser can directly access the domain renewal information and the security certificate information. | | | |
| 7. The firm's website is used to access client information. | | | |

| | | | |
|---|---|---|---|
| 8. SSL or other encryption is used when accessing client information on the firm's website. | | | |
| 9. The firm's website includes a client portal. | | | |
| 10. SSL or other encryption is used when accessing a client portal. | | | |
| 11. When accessing the client portal, user authentication credentials (i.e., user name and password) are encrypted. | | | |
| 12. Additional authentication credentials (i.e., challenge questions, etc.) are required when accessing the client portal from an unfamiliar network or computer. | | | |
| 13. The investment adviser has written policies and procedures related to a denial of service issue. | | | |
| **Protect: Custodians & Other Third-Party Vendors** | YES | NO | N/A |
| 1. The investment adviser's due diligence on third parties includes cybersecurity as a component. | | | |
| 2. The investment adviser has requested vendors to complete a cybersecurity questionnaire, with a focus on issues of liability sharing and whether vendors have policies and procedures based on industry standards. | | | |
| 3. The investment adviser understands that the vendor has IT staff or outsources some of its functions. | | | |
| 4. The investment adviser has obtained a written attestation from the vendor that it uses software to ensure customer data is protected. | | | |
| 5. The investment adviser has inquired whether a vendor performs a cybersecurity risk assessment or audit on a regular basis. | | | |
| 6. The cyber-security terms of the agreement with an outside vendor is <u>not</u> voided because of the actions of an employee of the investment adviser. | | | |
| 7. Confidentiality agreements are signed by the investment adviser and third-party vendors. | | | |
| 8. The investment adviser has been provided enough information to assess the cybersecurity practices of any third-party vendors. | | | |
| 9. [Relevant to custodians only] The investment adviser has discussed with the custodian matters regarding impersonation of clients and authentication of client orders. | | | |

| Protect: Encryption | YES | NO | N/A |
|---|---|---|---|
| 1. The investment adviser routinely consults with an IT professional knowledgeable in cybersecurity. | | | |
| 2. The investment adviser has written policies and procedures in place to categorize data as either confidential or non-confidential. | | | |
| 3. The investment adviser has written policies and procedures in place to address data security and/or encryption requirements. | | | |
| 4. The investment adviser has written policies and procedures in place to address the physical security of confidential data and systems containing confidential data (i.e., servers, laptops, tablets, removable media, etc.). | | | |
| 5. The investment adviser utilizes encryption on all data systems that contain (or access) confidential information. | | | |
| 6. The identities and credentials for authorized users are monitored. | | | |
| **Detect: Anti-Virus Protection and Firewalls** | YES | NO | N/A |
| 1. The investment adviser firm regularly use anti-virus software on all devices accessing the firm's network, including mobile phones. | | | |
| 2. The investment adviser firm regularly use anti-virus software on all devices accessing the firm's network, including mobile phones. | | | |
| 3. The investment adviser understands how the anti-virus software deploys and how to handle alerts. | | | |
| 4. The investment adviser understands how the anti-virus software deploys and how to handle alerts. | | | |
| 5. Anti-virus updates are run on a regular and continuous basis. | | | |
| 6. All software is scheduled to update. | | | |
| 7. Employees are trained and educated on the basic function of anti-virus programs and how to report potential malicious events. | | | |
| 8. If the alerts are set up by an outside vendor, there is an ongoing relationship between the vendor and the investment adviser to ensure continuity and updates. | | | |

| | | | |
|---|---|---|---|
| | | | |
| 9. A firewall is employed and configured appropriate to the firm's needs. | | | |
| 10. The firm has policies and procedures to address flagged network events. | | | |
| **Respond: Responding to a Cyber Event** | YES | NO | N/A |
| 1. The investment adviser has a plan and procedure for immediately notifying authorities in the case of a disaster or security incident. | | | |
| 2. The plans and procedures identify which authorities should be contacted based on the type of incident and who should be responsible for initiating those contacts. | | | |
| 3. The investment adviser has a communications plan, which identifies who will speak to the public/press in the case of an incident and how internal communications will be managed. | | | |
| 4. The communications plan identifies the process for notifying clients. | | | |
| **Recover: Cyber-insurance** | YES | NO | N/A |
| 1. The investment adviser has considered whether cyber-insurance is necessary or appropriate for the firm. | | | |
| 2. The firm has evaluated the coverage in a cybersecurity insurance policy to determine whether it covers breaches, including; breaches by foreign cyber intruders; insider breaches (e.g. an employee who steals sensitive data); and breaches as a result of third-party relationships. | | | |
| 3. The cybersecurity insurance policy covers notification (clients and regulators) costs. | | | |
| 4. The investment adviser has evaluated whether the policy includes first-party coverage (e.g. damages associated with theft, data loss, hacking and denial of service attacks) or third-party coverage (e.g. legal expenses, notification expenses, third-party remediation expenses). | | | |
| 5. The exclusions of the cybersecurity insurance policy are appropriate for the investment adviser's business model. | | | |
| 6. The investment adviser has put into place all safeguards necessary to ensure that the cyber-security policy is not voided through investment adviser employee actions, such as negligent computer security where software patches and updates are not installed in a timely manner. | | | |

| | | | |
|---|---|---|---|
| **Recover: Disaster Recovery** | YES | NO | N/A |
| 1. The investment adviser has a business continuity plan to implement in the event of a cybersecurity event. | | | |
| 2. The investment adviser has a process for retrieving backed up data and archival copies of information. | | | |
| 3. The investment adviser has written policies and procedures for employees regarding the storage and archival of information. | | | |
| 4. The investment adviser provides training on the recovery process. | | | |