PROPOSAL TO DEVELOP INDUSTRY BEST PRACTICES FOR TPSP CYBERSECURITY OVERSIGHT

Below are proposed components of a joint APCIA-CIAB project to develop voluntary industry best practices for assessment and monitoring of third-party service providers' (TPSPs) cyber risk and cybersecurity programs. New York currently has the most onerous requirements for TPSP cybersecurity oversight by insurance licensees, but we understand that other states may contemplate similar action in the future. The framework below, therefore, is intended to be adaptable for use in a multi-state or nationwide approach.

A. Develop Standardized Compliance Approaches Based on TPSPs' General Level of Risk to the Upstream Insurance Entity.

This risk-tiering approach builds on New York's existing cybersecurity regime to which many APCIA and CIAB members are subject. The goal is to develop standardized compliance protocols based on "bucketed" risk tiers for TPSPs. Each covered entity would decide into which tier each of its TPSPs falls. The compliance requirements for each tier would be based in part on whether a TPSP is a state-regulated entity with its own independent obligation to satisfy cybersecurity regulatory requirements, and whether there are other risk factors based on the relationship between the TPSP and the covered entity. For example, the compliance tiers could look something like the following:

1. *High Risk Tier: Specialized oversight protocol for state-regulated TPSPs.*

   - This tier would cover TPSPs that have their own independent obligation to adhere to a state's cybersecurity requirements as regulated businesses and to annually certify such compliance (e.g., NY-licensed entities subject to the NYDFS cyber rule), but are classified as high/higher risk by an upstream covered insurance entity due to unique access to that entity's data/systems, the nature or volume of the data held, and/or other criteria established by the covered entity.

   - Compliance requirements could include the TPSP's certification of full compliance with <u>all</u> state obligations (e.g., certification of compliance with all requirements under the NYDFS cyber rule), <u>PLUS</u> more frequent ongoing assessments by the covered entity, <u>PLUS</u> additional requirements tailored to the TPSP's unique situation and risk level.

2. *Medium Risk Tier: Standard oversight protocol based on <u>full</u> compliance with a state's cybersecurity regulations.*

   - This tier would cover TPSPs that have their own independent obligation to adhere to a state's cybersecurity requirements as regulated businesses and to annually certify such compliance (e.g., NY-licensed entities subject to the NYDFS cyber rule), but who present a moderate level of risk (e.g., no heightened or special risks) to the upstream insurance entity.

   - Compliance requirements could include the TPSP's certification of full compliance with <u>all</u> state obligations (e.g., certification of compliance with all requirements under the

NYDFS cyber rule), PLUS some ongoing verification/assessment by the upstream insurance entity.

3. *Low Risk Tier: Oversight protocol based on compliance with some subset of a state's cybersecurity regulations.*

    - This tier would cover smaller TPSPs that have their own independent obligation to adhere to some of a state's cybersecurity requirements as regulated businesses and to annually certify such compliance (e.g., NY-licensed entities subject to the NYDFS cyber rule), but who present a low level of risk (i.e., a lower than tiers 1 and 2) to the upstream insurance entity.

    - Compliance requirements could include the TPSP's certification of compliance with some subset of state obligations (e.g., certification of compliance with requirements for "small NY businesses" under the NYDFS cyber rule), PLUS some ongoing verification/assessment by the upstream insurance entity.

4. *Non-Regulated Tier: Oversight protocol for TPSPs not independently subject to a state's cybersecurity regulations.*

    - This tier would include, for example, non-NY-regulated vendors who do not have any independent obligation to comply with the NYDFS cybersecurity rule.

    - Compliance requirements would not be based on the TPSP's independent compliance with existing regulatory regimes, but would be directly imposed by the upstream insurance entity.

B. For Tiers **1, 2 and 3**, Develop a Common Form/Questionnaire for Initial Cyber Assessments of TPSPs.

We propose using APCIA's existing draft questionnaire as a starting point. The aim of this component would be to develop a standardized form so that state-regulated TPSPs (i.e. producers and carriers) can evaluate and respond to a single set of questions and distribute to all upstream insurance entities. Because use of the common form would be entirely voluntary, insurance entities that deploy it would be free to supplement the form with addendums as they deem necessary for the different levels of risk.

C. Develop a Standardized Ongoing Verification/Assessment Protocol for Tier **1, 2 and 3** TPSPs.

Similar to the initial cyber assessment questionnaire outlined in paragraph B above, we propose developing a common form/questionnaire for use in the periodic assessment of cyber risk and security programs of Tier 1, 2 and 3 TPSPs. We also propose establishing best practices with respect to the frequency of these assessments (e.g., annually, every two years, etc.). These ongoing assessments would be used to ascertain whether a TPSP's cyber program and/or risk level has materially changed, whether the TPSP should move risk tiers, etc. Absent a material change in law and/or circumstances of a TPSP, this likely would not be an active/full audit of a TPSP's cyber program or systems.

D. Potential Creation of Voluntary Standards/Best Practices for Assessments and Ongoing Oversight of Tier 4 Non-Regulated TPSPs.

This common structure could be used by insurance carriers and agents/brokers for their vendors who are not state-regulated businesses. If we were to develop such standards, we would invite some TPSPs in this category to participate in the process. We could explore developing common forms and common audit practices similar to those outlined above for Tiers 1, 2 and 3.