BIG I
NEW YORK

Using the checklist below, if you answer "**yes**" to any of the following questions, you should review and update, as necessary, your:

- Cybersecurity program
- Access privileges
- Data retention policy
- Cybersecurity policy
- Third party service provider security policy

SINCE YOUR LAST REVIEW, HAS YOUR AGENCY...?	YES	NO
Changed its computer systems by adding or changing any of the following: • Computer hardware (added or taken down workstations, servers, etc. that store nonpublic information) • Operating system (updated your version of Windows, switched to Mac, etc.) • Agency management system • Email provider or system • Application software • Copiers / printers • Telephone system • Security devices and applications (routers, firewalls, VPNs, encryption, multi-factor authentication, etc.) • Third-party data storage (e.g., "cloud storage) • Mobile devices (phones, tablets) owned by the agency or employees • Rules for changing network passwords • Procedures for ending network access for separated employees	☐	☐
Moved to a new physical location	☐	☐
Opened or closed satellite offices	☐	☐
Purchased any other agencies or their books of business	☐	☐
Merged with another agency	☐	☐
Started offering new lines of coverage (commercial, life, benefits, etc.)	☐	☐
Started offering non-insurance services	☐	☐
Added new functions to its website	☐	☐
Started or stopped representing any carriers	☐	☐
Started or stopped working with any wholesale brokerages or managing general agencies	☐	☐
Grown to the point where you have separate staff for functions such as billing, claim handling, underwriting, IT, etc.	☐	☐
Made a major change in marketing strategy (focus on specific niches, high net worth households, etc.)	☐	☐
Changed errors and omissions liability insurance carriers	☐	☐
• If "**YES**," does the new carrier require the agency to implement new cybersecurity controls	☐	☐
Implemented or updated a disaster recovery plan	☐	☐
Suffered a data breach or malware attack that your current program did not contain	☐	☐
Suffered a phishing attack that had an adverse impact on your business	☐	☐