PENNSYLVANIA GAMING CONTROL BOARD
P.O. BOX 69060
HARRISBURG, PENNSYLVANIA
17106-9060

PAUL RESCH
Director, Bureau of Gaming Operations
303 Walnut Street
Commonwealth Tower
5th Floor, Strawberry Sq.
Harrisburg, PA 17101
Phone: (717) 346-8300
Fax: (717) 346-8350
Email: presch@pa.gov
Website: gamingcontrolboard.pa.gov

October 25, 2021

Sent via Electronic Mail

Interactive Gaming Certificate Holders
Interactive Gaming Operators
Interactive Gaming Manufacturers
Sports Wagering Certificate Holders
Sports Wagering Operators

Re: Interactive Gaming System Security Audit

Dear Interactive Gaming Stakeholder:

The purpose of this letter is to provide guidance on the interactive gaming system security audit requirements established by the Pennsylvania Gaming Control Board ("Board") in 58 Pa. Code § 809a.6(d) and as described in the Board's Release Notes Guidelines. This guidance is applicable for interactive gaming certificate holders and operators, sports wagering certificate holders and operators and interactive gaming manufacturers (hereinafter "operators").

Operators must perform an annual security audit within 90 days of commencing operations and then by launch date annually thereafter. It is acceptable for the initial security audit to be submitted to the Board no later than 120 days after launch to allow licensees adequate time to evaluate the results and provide a response and/or remediation plan. Initial security audits are required for operators that commence operations on or after October 25, 2021. Annual security audits will be required beginning April 1, 2022 for operators that commenced operations on or after April 1 in a prior year. For example, a licensee that commenced operations on May 31, 2019 is required to submit an annual security audit by May 31, 2022.

The security audit must be performed by an independent third-party cyber security company selected by the operator, subject to Board approval. The scope of the security audit is subject to Board approval and must include, at a minimum, the following:

- Application penetration test (mobile and web)
- Internal vulnerability assessment and penetration test
- External vulnerability assessment and penetration test
- Information security management system audit (GLI-33 B/GLI-19 B or other applicable security framework)

In addition, and as applicable, the security audit must include a data security review to ensure the following player data is encrypted or hashed as required by 58 Pa. Code § 812a.2(d):

- Any portion of the patron's Social Security Number or equivalent for a foreign patron such as a passport or taxpayer identification numbers
- Patron passwords and/or personal identification numbers
- Credit card numbers, bank account numbers or other personal financial information (For operators that do not retain and/or store this financial information and rely upon the services of authorized payment providers, the operators shall provide an attestation to the Board in which they attest that the financial information is not retained or stored on its system.)

In addition to the security audit report, operators must provide a remediation plan to include the following:

- Vulnerability name and description
- Severity rating
- Action to be taken
- Planned date of completion
- Actual date of completion

Operators must update the remediation plan as milestones are completed and submit to the Board.

Prior to performing the initial or annual security audit, operators must submit the name of the third-party service provider that will perform the audit and a proposed scope of work to the Board for approval. In addition, operators must submit a Gaming Service Provider iGaming/Sports Wagering Notification form and receive authorization from the Bureau of Licensing. If the third-party cyber security company utilizes a subcontractor to perform part of its audit (e.g., external scans of the system), operators must also submit a Gaming Service Provider iGaming/Sports Wagering Notification form on behalf of the subcontractor and receive authorization from the Bureau of Licensing.

Operators must also perform internal and external network vulnerability scans on a quarterly basis. Operators must provide credentialed vulnerability scans of all systems that comprise the interactive gaming system. For operators, especially interactive gaming manufacturers that maintain multiple clients (i.e., tenants) in the same system, those operators and their clients may propose a quarterly vulnerability scan process to the Board that limits the filing of multiple reports with the same vulnerability findings. These quarterly scans can be performed by a third-party service provider or a qualified employee of the operator as approved by the Board. If a third-party service provider will perform the scans, operators must submit the Gaming Service Provider Notification form noted above. Testing procedures must verify that rescans occurred until all "medium risk" (CVSS 4.0 or higher) vulnerabilities identified in that quarterly scan were resolved. Any additional vulnerabilities identified in the rescans should be carried over into the next quarterly report. Executive summary reports from the quarterly scans must be submitted to the Board by the end of each calendar quarter. The full detailed

vulnerability scans must be available upon request. A remediation plan must include the following:

- Vulnerability name and description
- Severity rating
- Action to be taken
- Planned date of completion
- Actual date of completion

The operator must update the remediation plan as milestones are completed and submit to the Board. The first quarterly scan report is due March 31, 2022.

Board staff are developing an iGaming customer service portal that operators will use to securely transmit the required reports. It is anticipated those portal services will be available by April 1, 2022. Additional information, including login credentials, will be provided to operators when the portal services are available. In the meantime and until further notice, operators are advised to submit the reports to ITsecurityPGCB@pa.gov.

If you have any questions regarding the security requirements, please contact Paul Resch, Director of Gaming Operations, at (717) 214-4736 or presch@pa.gov. If you have any questions about licensing of third-party service providers, please contact Mark Miller, Manager, Bureau of Licensing, Gaming Service Provider Unit, at (717) 703-2817 or mmillerrev@pa.gov.

Sincerely,

Paul Resch
Director, Bureau of Gaming Operations

cc: Kevin F. O'Toole, Executive Director, PGCB
Stephen Cook, Acting Chief Counsel, PGCB
Claire Yantis, Administrative Director, PGCB
Cyrus Pitre, Chief Enforcement Counsel, PGCB
Paul Mauro, Director, Bureau of Investigations & Enforcement, PGCB
Sean Hannon, Director, Bureau of Licensing, PGCB
Heather Worner, Director, Bureau of Gaming Laboratory Operations, PGCB
Paul Resch, Director, Bureau of Gaming Operations, PGCB
Kevin Kile, Director of Sports Wagering Operations, PGCB
Stephen Dunn, Director of Information Technology, PGCB
Mark Miller, Manager, Bureau of Licensing, PGCB