Title 36 MARYLAND STATE LOTTERY AND GAMING CONTROL AGENCY

Subtitle 10 SPORTS WAGERING PROVISIONS

Chapter 18 Sports Wagering Technical Standards

Authority: State Government Article, §§9-1E-01—9-1E-15, Annotated Code of Maryland

.06 Information Security.

A. A sports wagering licensee shall:

(1) Implement, maintain, regularly review and revise, and comply with a comprehensive information security system that reasonably protects the confidentiality, integrity, and availability of a bettor's personally identifiable information; and

(2) Ensure that the security system set forth in §A(1) of this regulation includes administrative, technical, and physical safeguards which:

(a) Are appropriate to the size, complexity, nature, and scope of the operations; and

(b) Protect the personal information owned, licensed, maintained, handled, or otherwise in the possession of the sports wagering licensee.

B. A sports wagering licensee shall:

(1) Within 90 days of commencing operations, and annually thereafter, conduct a vulnerability assessment, penetration testing, and operational security control review against ISO 27001 standard, or other similar standards such as CIS or NIST CSF;

(2) Perform vulnerability assessments and penetration testing of the sports wagering platform at multiple layers, including:

(a) Internal and external network;

(b) Mobile and web application;

(c) Database;

(d) Firewall;

(e) If applicable, wireless; and

(f) Any additional security testing that the Commission requires;

(3) Ensure that a Commission approved third party described in Regulation .02B of this chapter conducts the testing required in §B(1) and (2) of this regulation; ~~and~~

PROPOSED

(4) Ensure that the annual reporting required in §B(1) - (3) of this regulation is submitted to the Commission no later than 120 days after the end of the licensee's fiscal year; and

(**5**) Perform internal quarterly vulnerability scans, and ~~retain~~ **submit to the Commission** documentation of the scan results and the actions taken to resolve identified vulnerabilities.

C. A sports wagering licensee shall submit to the Commission the assessment report issued by the third party and the licensee's report.

D. The ~~combined~~ reports in §C of this regulation shall:

(1) Provide details for all vulnerabilities identified;

(2) Assess the adequacy and effectiveness of the sports wagering licensee's information technology security controls and system configurations; and

(3) Provide recommendations for eliminating each material weakness or significant deficiency identified.

E. A sports wagering licensee shall evaluate all identified vulnerabilities for potential adverse effect on security and integrity and:

(1) Remediate the vulnerability no later than 90 days following the earlier of vulnerability's identification or public disclosure; or

(2) Document why remediation action is unnecessary or unsuitable.

PROPOSED