205 CMR 243.00: SPORTS WAGERING EQUIPMENT

243.01: Standards for Sports Wagering Equipment

(1) A Sports Wagering Operator and Sports Wagering Vendor shall comply with, and the commission adopts and incorporates by reference, *Gaming Laboratories International, LLC Standard GLI-33: Event Wagering Systems* and its appendices, version 1.1, released May 14, 2019, subject to the following amendments:

(a) Delete section 1.1.1 and replace with the following: "The following sets forth the technical standards for sports wagering equipment as identified in 205 CMR 244.01."

(b) Delete section 1.1.2.

(c) Delete section 1.2.1.

(d) Delete section 1.3.3 and replace with the following: "This GLI technical standard is adopted in whole, subject to the modifications described in 205 CMR 243.01. To create a congruent regulatory framework, the standard and modifications should always be read in conjunction with 205 CMR and the standards reference in section 1.4.1."

(e) Add the following after section 2.1.1 "and the modifications described in 205 CMR 243.01."

(f) Delete the second sentence of section 2.5.1 and replace with the following: "In addition to the requirements contained within this section, and 205 CMR, the "Player Account Controls" section of this document shall also be met."

(g) Delete section 2.5.6(b) and replace with the following: "A deposit into a player account shall not be made using a credit card and must be made by methods which can produce a sufficient audit trail."

(h) Delete from section 2.7.1 the words "Where required by the regulatory body"

(i) Add the following at the end of section 2.7.4: "All wagers must be initiated and received or otherwise made by an individual located in the Commonwealth. Consistent with the intent of the federal Unlawful Internet Gambling Enforcement Act of 2006, 31 U.S.C. section 5361 to 5367, inclusive, the intermediate routing of electronic data related to a lawful intrastate wager authorized pursuant to M.G.L. c. 23N shall not determine the location or locations in which the wager is initiated, received, or otherwise made."

(j) Replace in section 2.7.4(a) the words "or as otherwise specified by the regulatory body" with "after a period of 5 minutes since the previous location check if within one mile of the border, and prior to placement of the next wager after detection of a change to the player's IP Address"

(k) Add the following as section 2.7.4(e): "The location detection service or application used by the Event Wagering System shall be certified by the approved Independent Testing Laboratory, including applicable field testing, before its deployment."

(l) Delete section 2.8.2(o) and replace with the following: "(o) The personally identifiable information of a player who places a wager that exceeds $10,000 or wins a wager exceeding $600 and is 300 times the amount wagered including, the legal name, residential address, date of birth, and encrypted government identification number (full or partial social security number, taxpayer identification number, passport number, or equivalent)."

(m) Delete from section 2.8.5(j)(ix) the words "or credit"

(n) Replace in section 2.8.8(d) the words "a value specified by the regulatory body" with "$10,000, or $600 and is 300 times the amount wagered"

(o) Replace in section 2.8.8(e) the words "a value specified by the regulatory body" with

"$10,000"

(p) Replace in section 2.8.8(n)(iv).the words "a value specified by the regulatory body" with "$10,000"

(q) Add the following as section 2.9.1(c): "The operator shall timely file with the commission the reports required by this section in accordance with M.G.L. c. 23N, § 12(a)(ix) and 205 CMR."

(r) Replace in section 3.3.1 the words "other applicable jurisdictional requirements observed by the regulatory body" with "the modifications described in 205 CMR 143.07"

(s) Add the following as section A.1.2: "A.1.2 Independent Audit. Each operator shall have their procedures and practices for wagering operations independently audited at least once every two (2) years with the results documented in a written report. Reports shall be maintained and available to the commission upon request. An operator's audit practices shall include, but not be limited to, the following:

a) Independent audits may be conducted by the commission, or a commission approved third-party auditor. The commission may, in its discretion, allow for an internal audit department within the operator or parent company of the operator, which is independent of the wagering operation, to serve as a third-party auditor for use in completing this audit.

b) The commission, or third-party auditor shall be responsible for auditing the operator's compliance with M.G.L. c. 23N, 205 CMR, this appendix, the internal control system, and any other applicable rules and regulations.

c) Documentation, including checklist, programs, reports, corrective actions, and other items, shall be prepared to evidence all independent audit work performed as it relates to the requirements of 205 CMR 243.01 and this appendix, including all instances of noncompliance.

d) Independent audit reports shall include objectives, procedures and scope, findings and conclusions, and recommendations.

e) Independent audit findings shall be reported to management. Management shall be required to respond to the independent audit findings and the stated corrective measures to be taken to avoid recurrence of the audit exception. Such management responses shall be included in the final independent audit report.

f) Follow-up observation and examinations shall be performed to verify that corrective action has been taken regarding all instances of noncompliance cited by the independent audits, or by the commission. The verification shall be performed within six (6) months following the date of notification.

g) It is acceptable to leverage the results of prior audits conducted within the audit period by the same third-party auditor in another jurisdiction. Such leveraging shall be noted in the audit report. This leveraging does not include any procedures and practices unique to the Commonwealth, which will require new audits."

(t) Add the following at the end of section A.2.1: "The internal control procedures shall meet the requirements of this appendix and 205 CMR 238."

(u) Replace in section A.4.5 the word "credit card" with "financial"

(v) Delete section A.7.4(d) and replace with the following: "(d) Is kept for at least one year after a sporting event occurs."

(w) Delete from section A.8.3 the words "where required by the regulatory body"

(x) Add the following as section B.1.2: " B.1.2 Independent Audit. The operator shall, within

ninety (90) days after commencing operations in the Commonwealth, and annually thereafter, have a technical security control audit conducted by a qualified independent technical expert selected by the operator and subject to approval of the commission. The commission will establish minimum qualifications for technical experts, to be published on its website, which must be reviewed and updated annually.

a) The scope of the technical security control audit is subject to approval of the commission or its designee and must include, at a minimum, all of the following:
   i. A vulnerability assessment of all digital platforms, mobile applications, internal, external, and wireless networks with the intent of identifying vulnerabilities of all devices, the servers, and applications transferring, storing, and/or processing personally identifiable information and/or other sensitive information connected to or present on the networks.
   ii. A penetration test of all digital platforms, mobile applications, internal, external, and wireless networks to confirm if identified vulnerabilities of all devices, the servers, and applications are susceptible to compromise.
   iii. A review of the firewall rules to verify the operating condition of the firewall and the effectiveness of its security configuration and rule sets performed on all the perimeter firewalls and the internal firewalls;
   iv. An information security assessment against the provisions adopted in M.G.L. c. 23N, 205 CMR, this appendix with generally accepted professional standards and as approved by the commission;
   v. If a cloud service provider is in use, an assessment performed on the access controls, account management, logging and monitoring, and over security configurations of their cloud tenant;
   vi. An evaluation of information security services, payment services (financial institutions, payment processors, etc.), location services, and any other wagering services which may be offered directly by the operator or involve the use of third parties against the provisions adopted in these rules; and
   vii. Any other specific criteria or standards for the technical security control audit as prescribed by the commission or its designee.
b) To qualify as an independent technical expert, the independent technical expert shall:
   i. Have relevant education background or in other ways provide relevant qualifications in assessing Event Wagering Systems;
   ii. Obtain and maintain certifications sufficient to demonstrate proficiency and expertise as a network penetration tester by recognized certification boards, either nationally or internationally;
   iii. Have at least five years' experience performing technical security control audits on Event Wagering Systems; and
   iv. Meet any other qualifications as prescribed by the commission or its designee.
c) The full independent technical expert's report on the assessment must be submitted to the commission no later than thirty (30) days after the assessment is conducted and must include all the following:
   i. Scope of review;
   ii. Name, company affiliation, contact information, and qualifications of the individual(s) who conducted the assessment.
   iii. Date of assessment;

iv. Findings;
v. Recommended corrective action, if applicable; and
vi. The operator's response to the findings and recommended corrective action.

d) It is acceptable to leverage the results of prior assessments within the past year conducted by the same independent technical expert in another jurisdiction or against standards such as ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, the NIST Cybersecurity Framework (CSF), the Payment Card Industry Data Security Standards (PCI-DSS), or equivalent. Such leveraging shall be noted in the independent technical expert's report. This leveraging does not include critical components unique to the Commonwealth which will require fresh assessments.

e) If the independent technical expert's report recommends corrective action, the Sports Wagering Operator must provide the commission with a remediation plan and any risk mitigation plans which detail the operator's actions and schedule to implement the corrective action. Once the corrective action has been taken, the Sports Wagering Operator shall provide the commission with documentation evidencing completion."

(y) Replace the paragraph in B.2.2 with the following: "The Sports Wagering Operator shall provide the commission with information on the secure locations of all servers and other equipment used for Sports Wagering for its approval. Unless otherwise approved by the commission, the primary server or other equipment responsible for the acceptance of sports wagers shall be placed in secure locations within the Commonwealth. In addition, secure location(s) shall:"

(z) Replace section B.4.5 with the following: B.4.5 Communications in Wagering Venues. If a guest network is offered that provides internet access for players, venue guests, or vendors, the guest network must be physically or logically segregated from the network used to serve the Event Wagering System. Communications on the guest network must be non-routable to the Event Wagering System network.

(aa) Delete from section B.7.6 the words "If required by the regulatory body"

(bb) Add the following to the beginning of section B.9.5: "The commission may approve of the use of internet or cloud-based hosting of duplicate data or data not related to transactional wagering data upon written request of the operator."