GLI®

World Headquarters

600 Airport Road
Lakewood, NJ 08701

Phone (732) 942-3999
Fax (732) 942-0043
www.gaminglabs.com

January 24, 2020

Mr. Lyndon Bennett
NYX Digital Gaming (Alberta) Ltd
4300 Bankers Hall West, 888 – 3rd Street, S.W.
Calgary AB T2P 5C5

RE: Random Number Generator Report

Dear Mr. Bennett:

Enclosed, please find a detailed explanation of the Random Number Generator (RNG) testing results of the NYX Digital Gaming (Alberta) Ltd OGS RNG, evaluated against the RNG-specific requirements listed herein.

Please visit Gaminglabs.com to view the applicable Terms and Conditions.

If you should have any questions regarding this information, please feel free to contact our office.

Sincerely,
GAMING LABORATORIES INTERNATIONAL, LLC

Christine M. Gallo
Vice President of Technical Compliance and Quality Assurance

RN-385-NYX-19-01

ENCLOSURES

ld

Worldwide Locations

World Headquarters
Lakewood, New Jersey

U.S. Regional Offices
Colorado
Nevada

International Offices
GLI Africa
GLI Asia
GLI Australia Pty Ltd
GLI Austria GmbH
GLI Europe BV
GLI Italy
GLI South America

RANDOMNESS REPORT FOR THE NYX DIGITAL GAMING (ALBERTA) LTD OGS RNG

The intent of this report is to indicate that **Gaming Laboratories International, LLC** (GLI) has completed its evaluation of the OGS random number generator (RNG), provided by NYX Digital Gaming (Alberta) Ltd.

SECTION I – SCOPE OF TESTING

The OGS RNG was assessed for suitability for use in gaming applications through static analysis of source code and statistical analysis of data generated using the supplied test utility.

The analysis undertaken is intended to confirm that the implementation and instantiation methods comply with the requirements of the jurisdiction in the scope of this assessment.

The OGS RNG was evaluated against the RNG-specific requirements of the following technical standards:

- Remote Gambling and Software Technical Standards (June 2017)
- Testing Strategy for Compliance with Remote Gambling and Software Technical Standards November 2018

SECTION II – SOFTWARE VERIFICATION

Verify+ by Kobetron™ signatures for the OGS RNG are as follows:

File	Type	Signature
libswrng.so	Kobe4	4654
	MD5	547E0ADAB2B2929ADAB2A2864CDD5F25
	SHA-1	7D1C8B29688D3E8EDD723E19DACD316ABCDCCB82

Table 1. Digital Signatures

SECTION III – SOURCE CODE REVIEW

NYX Digital Gaming (Alberta) Ltd submitted appropriate documentation and full source code which pertains to the generation of random numbers. GLI reviewed the source code and assessed the ability of the RNG to produce all numbers within the desired range.

SECTION IV – DATA ANALYSIS

GLI conducted a statistical analysis of sufficient scope to test the RNG, as described in Table 2. To provide this level of assessment, GLI selected 8 different test cases for statistical testing. The selection of test cases took into account broad coverage of range sizes and selections.

A set of numbers is said to be drawn *with replacement* if a number can be selected multiple times within the same draw. A set of numbers is said to be drawn *without replacement* if a number can only be selected once within the same draw.

Data Set	Range	Positions	Replacement	Draws
Data Set 1	0 - 2^32 - 1 (inclusive)	1	No	32,000,000
Data Set 2	0 - 2^32 - 1 (inclusive)	1	No	9,000,000
Data Set 3	0 - 36	1	No	40,000,000
Data Set 4	0 - 51	1	No	40,000,000
Data Set 5	0 - 126	1	No	50,000,000
Data Set 6	0 - 255	1	No	50,000,000

Table 2. Ranges Tested

For a summary of the statistical tests applied to each data set, see *Appendix A*. For a description of the overall test methodology and a description of each test used, see *Appendix B*.

Overall, the RNG passed the battery of tests for each configuration at the 95% and 99% confidence levels.

SECTION V - SUMMARY

Overall Evaluation of the Random Number Generator

GLI's conclusion based upon the tests applied to the NYX Digital Gaming (Alberta) Ltd OGS RNG data is that this RNG has exhibited random behavior and is suitable for the applications as described herein.

APPENDIX A: Statistical Test Summary

					Test Names							
Data Set	**Range**	**Positions**	**Replacement**	**Draws**	**Frequency Test**	**Serial Test**	**Gap Test**	**Poker Test**	**Permutations Test**	**Run Test**	**Diehard Battery of Tests**	**NIST Test Suite**
Data Set 1	0 - 2^31 - 1 (inclusive)	1	No	32,000,000								X
Data Set 2	0 - 2^31 - 1 (inclusive)	1	No	9,000,000							X	
Data Set 3	0 - 36	1	No	40,000,000	X	X	X	X	X	X		
Data Set 4	0 - 51	1	No	40,000,000	X	X	X	X	X	X		
Data Set 5	0 - 126	1	No	50,000,000	X	X	X	X	X	X		
Data Set 6	0 - 255	1	No	50,000,000	X	X	X	X	X	X		

Table A 1. Tests Applied

APPENDIX B: Test Descriptions

B.1 **Definitions.** The following terms apply to the below test descriptions. Randomness Device or Random Number Generator (RNG) output may be collected multiple numbers at a time. Each set of numbers is called a draw. Each individual number has a particular order within the *draw*. This is referred to as the number *position*.

B.2 **Distribution Comparisons.** Many of the tests compare an observed numerical distribution with an expected distribution. Unless otherwise specified, this is done by means of a statistical chi-square goodness-of-fit test. The value chi-square is computed in the standard way. If *k* is a possible value, o_k is the observed count of that value, and e_k is the expected count:

$$\chi^2 = \sum_k \frac{(o_k - e_k)^2}{e_k}$$

In the case where expected counts are too small for accurate use of the above formula, values are 'binned' together to ensure an appropriate minimum expected count. The resultant value for chi-square is compared against the distribution for the appropriate number of degrees of freedom. Unusually high (distribution mismatch) or unusually low (insufficient randomness) chi-square values can be causes for data failure.

B.3 **Meta-testing**. Evaluation of groups of *p*-values may include a meta-test for extremity of high or low *p*-values, a meta-test for frequency of high or low *p*-values, and a meta-test for uniformity of *p*-values, as appropriate.

B.4 **Confidence Level**. The statistical tests conducted by GLI are done at a particular *confidence level*. Common confidence levels used include 95%, 98%, and 99%, depending on jurisdictional requirements, and intended use of the RNG. High confidence level testing has low risk of mistakenly failing a good RNG, but higher risk of passing a bad RNG. Lower confidence level testing has increased power of detecting bad RNGs, while also increasing the risk of false failures of good RNGs. Specifically, the confidence level represents the probability that an ideal source of randomness would pass the testing. If an RNG passes statistical tests at a given confidence level, passage at all *higher* confidence levels is implied.

B.5 **Tests**. Some tests are only applicable to certain types of data. Some tests may be applied only to a portion of the data. Some tests may require that the data be parsed, binned, or otherwise transformed, as necessitated by data format.

<u>Test Suites:</u>

NIST Test Suite
The following “bitwise” tests from the NIST Test Suite were applied:

- Frequency (Monobits) Test
- Frequency Test within a Block
- Runs Test
- Test for the Longest Run of Ones in a Block
- Binary Matrix Rank Test
- Discrete Fourier Transform (Spectral) Test
- Non-overlapping Template Matching Test
- Maurer’s “Universal Statistical” Test
- Linear Complexity Test
- Serial Test
- Approximate Entropy Test
- Cumulative Sums (Cumsum) Test
- Random Excursions Test
- Random Excursions Variant Test

Diehard Battery of Tests
The following “bitwise” tests from the Diehard Battery of Tests of Randomness were applied:

- Birthday Spacing Test
- Overlapping 5-permutations Test
- Binary Rank 31x31 Test
- Binary Rank 32x32 Test
- Binary Rank 6x8 Test
- Bitstreams Test
- Overlapping Pairs Sparse Occupancy (OPSO) Test
- Overlapping Quadruples Sparse Occupancy (OQSO) Test
- DNA Test
- Count the 1’s (Specific Bytes) Test
- Count the 1’s (Stream of Bytes) Test
- Parking Lot Test
- Minimum Distance Test
- 3-D Spheres Test
- Squeeze Test
- Overlapping Sums Test
- Runs Test
- Craps Test

Donald Knuth's Empirical Tests for Randomness

The following tests were applied to the scaled and shuffled RNG outputs:

- Frequency Test (Equidistribution Test)
- Serial Test (Non-overlapping Pairs)
- Gap Test
- Poker Test (Partition Test)
- Permutation Test
- Runs Test

All test results are based on the Pearson chi-squared test (also known as the chi-square "goodness of fit" test) to compare the observed results against expected outcomes and determine a level of confidence. For the following test descriptions, assume that a number n of uniformly distributed random numbers on the range [0, m-1], with m being an amount of distinct outcomes, were generated.

<u>Test Descriptions:</u>

Frequency Test

The Frequency Test is designed to ensure that the random numbers are uniformly distributed throughout a given interval. The instances of each number in the range [0, *m*-1] are counted and the counts compared to the expected populations. The probability *P* of observing any particular number *x* in a given position in the sequence is:

$$P(x) = \frac{1}{m}, \quad 0 \leq x \leq m - 1.$$

The variation in observed distribution against the theoretical value is used to calculate the chi-squared statistic. The value of chi-squared statistic then maps to a probability (i.e. a p-value) that provides a measure of confidence in the observed outcomes.

Serial Test

The Serial Test checks that pairs of numbers are uniformly distributed in an independent manner. The random numbers are distributed into a number of equal bins and the frequencies of occurrence of all possible sequence pairs are checked (i.e. 0 followed by 0, 0 followed by 1, ..., *m*-1 followed by *m*-1). If the numbers are uncorrelated (i.e. no sequence pairs are favored over any others), an equal distribution is expected and the probability of observing a sequence *(x,y)* is equal to:

$$P(x, y) = \frac{1}{m^2}, \quad 0 \leq x, y \leq m - 1.$$

Similar to the frequency test, the observations and theoretical probabilities are used to compute a chi-squared statistic, which is then used to determine a probability that all serial pairs are uniformly distributed.

Gap Test

The Gap Test considers the length of "gaps" between occurrences of specific numbers (i.e. the average gap between an occurrence of the number "1" and the next occurrence of "1" should be the same as that between a "2" and the next "2"). To apply the gap test, the lengths of the gaps between occurrences of a particular number are collated and the frequencies of occurrence are compared with the expected counts for each gap size. If subsequent numbers in the sequence are random and independent, the probability of a gap of length *g*, between instances of a particular output with probability $p = 1/m$, occurring is:

$$P(g) = p(1-p)^g$$

All gaps larger than a pre-determined threshold are grouped into a single category and counted. The probability of observing a gap of length *u* or larger is:

$$\sum_{g=u}^{\infty} P(g) = (1-p)^u$$

A comparison of the observed and the expected gap sizes (via the chi-squared test) is then applied to assess if the sequence was generated by a sufficiently random source.

Poker Test

The Poker Test uses the analogy of a five-card hand in a poker game. It considers groups of five successive integers and observes which of the following 5 patterns is matched by each quintuple:

- 5 values (all different)
- 4 values (one pair)
- 3 values (two pairs or three of a kind)
- 2 values (full house or 4 of a kind)
- 1 value (five of a kind)

If each individual outcome is equally probable, the probability of achieving *v* distinct outcomes (in a group of *k* outcomes with *d* possible outcomes) is given by:

$$P(v) = S(k,v) \times \left(\frac{d(d-1)\dots(d-v+1)}{d^k} \right)$$

where *S(k,v)* is the Stirling Number of the second kind (the number of ways to partition a set of *k* elements into *v* non-empty subsets). To apply the Poker test, the generated random numbers are gathered into groups and categorized according the patterns listed above. The counts of each categorization are compared with expected values via the chi-squared test.

Permutations Test
The Permutations Test divides a number sequence with a range of *m* elements into *n* groups of *t* elements. In this specific application, groups of $t = 3$ numbers were considered (denoted *a*,*b*,*c*) and counted the occurrence of each of the 6 different relative orderings:

- $a < b < c$
- $a < c < b$
- $b < a < c$
- $b < c < a$
- $c < a < b$
- $c < b < a$

The cases where two or more of the three numbers in a group are equal are also counted. The probability P^* that two or more of the instances are equal is given by:

$$P^* = \frac{1}{m} + \frac{2(m-1)}{m^2}$$

Hence, the probability of observing any of the listed permutations (*lp*) is:

$$P(lp) = \frac{(1 - P^*)}{3!}$$

A chi-squared test is conducted to test whether the observed counts of the permutations (including the matching cases) is consistent with the theoretical distribution.

Runs Test
A sequence of random numbers will typically contain sub-sequences in which the numbers are increasing (they "run up") and sub-sequences in which they are decreasing (they "run down"). In this test, the sequence is split into segments in which the length is determined by whether or not the next number is higher (in the case of "run up") or lower (in the case of "run down"). The number immediately following a run is discarded in order to make runs independent and make the chi-square test applicable. The observed value is then compared with the theoretical value and a level of confidence is calculated.

Consider a sequence of uniformly distributed random numbers with *m* possible individual outcomes. The expected probability of a run of *r* consecutive numbers is:

$$P(r) = \begin{cases} m^{-r}\binom{m}{r} - m^{-(r+1)}\binom{m}{r+1} & \text{if } 0 < r < m \\ m^{-m} & \text{if } r = m. \end{cases}$$

The number of independent runs of each length up to and including *m* are compiled and compared with the expected values via a chi-squared goodness-of-fit test.

References:

- Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S. (2010) *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [Online] Rev. 1a. Gaithersburg, MD, USA. National Institute of Standards & Technology.
- Knuth, D. (1997). The Art of Computer Programming. Volume 2: Seminumerical Algorithms. 3rd ed. Boston: Addison-Wesley Longman Publishing Co, Inc.