



WISCONSIN LOTTERY

  Find us at wilottery

Department of Revenue
2135 Rimrock Road
P.O. Box 8941
Madison, Wisconsin 53708-8941
wilottery.com

FOR IMMEDIATE RELEASE

October 9, 2015

CONTACT: Lottery Communications, 608.266.2300

Wisconsin Lottery Asks Wisconsin Department of Justice to Review December 2007 Megabucks Lottery Draw

MADISON – The Wisconsin Lottery has asked the Wisconsin Department of Justice to review the December 29, 2007, Megabucks drawing to determine if any illegal activity may have occurred. The Lottery made this request because a vendor's employee who had access to Wisconsin's random number generators (RNGs) has allegedly also committed fraud in Iowa and Colorado. The drawing machines used in 2007 are no longer in use, and earlier this year, an independent auditing firm confirmed the integrity of the Wisconsin Lottery's current gaming systems.

"We asked the Department of Justice to look into a December 2007 drawing to determine if any illegal activity occurred in Wisconsin," said Lottery Director Mike Edmonds. "At this time, we have no other suspicions than the December 2007 drawing, and we know DOJ will be vigilant in its review. Protecting the integrity of our games is of utmost importance, and third party independent validators have confirmed the integrity and security of the Lottery's current random number generators."

Iowa Allegations

According to an Iowa criminal complaint issued on October 8, 2015, Eddie Tipton was convicted in July 2015 on two counts of fraud for his participation in a scheme to collect on a \$16.5 million Hot Lotto ticket from a winning jackpot in December 2010 (the Hot Lotto game is not played in Wisconsin). Tipton, who had access to the machines used to pick lottery numbers because of his role in providing software updates as a Multi-State Lottery (MUSL) employee, was accused of rigging the Hot Lotto game to produce predetermined numbers on a specific date. Tipton then later purchased a Hot Lotto ticket with those predetermined numbers in December 2010 and won the jackpot on December 29, 2010. Tipton is appealing those convictions.

Today, the Iowa Attorney General announced new charges against Tipton. He is charged with Ongoing Criminal Conduct for an alleged scheme in defrauding lotteries in Iowa, Wisconsin and Colorado.

Wisconsin Review

In September 2015, the Wisconsin Lottery asked the Wisconsin Department of Justice to review the December 29, 2007, Megabucks drawing in which a "Robert Rhodes" claimed the \$2 million jackpot prize on February 26, 2008. The ticket was brought to the Lottery's Madison headquarters by an attorney for Rhodes. It was signed by Robert Rhodes of Sugar Land, Texas, with the prize payable to Delta S Holdings, LLC.

State law requires the Lottery to pay a prize to an individual, unless otherwise directed by the courts to pay to a trust. The winner chose the lump sum cash payment of \$1,147,630 and was paid \$783,257 after taxes to Delta S Holdings, LLC following a Dane County Court Order.

October 9, 2015

Page Two

"If it is determined that something illegal took place, we will pursue a criminal prosecution, which will include demanding repayment of the funds," said Edmonds.

The Lottery's drawing machines are independent devices that are not connected to a network. They are kept on a locked floor, in a locked room, surrounded by a sealed locked case, and all drawings are witnessed by a Certified Public Accountant (CPA) and security to ensure all the proper protocols and internal controls are in place when conducting drawings.

In June 2015, the Lottery also had an independent third party validator, Digital Intelligence (DI), review the three random number generators that were installed in 2014 as an additional precaution. Digital Intelligence provides forensic casework and analysis for law enforcement, intelligence organizations and other corporate security professionals. The RNGs had already been certified in May 2014 by BMM Testlabs as accurately generating random numbers that are unbiased and unpredictable. The BMM Testlabs review also stated that the RNGs do not contain any malicious code.

Digital Intelligence examined the systems to identify unusual, questionable or suspect activity or files on any of the computers. After comprehensive evaluation and testing, DI reached the conclusion that there is no "...unusual, questionable or suspect activity on the RNG computer systems in use by the Wisconsin Lottery." DI also did not identify any malicious files or malware.

- END -

BMM CERTIFICATION TEST REPORT

Report Issue Date: 7th May, 2014

Issued To: Multi-State Lottery Association

Issued By: BMM Testlabs
[REDACTED]
815 Pilot Road, Suite G, Las Vegas, NV 89119
(702) 407 2420, www.bmm.com

Compliance Tested By: BMM Testlabs
815 Pilot Road, Suite G
Las Vegas, NV 89119

Manufacturer: Multi-State Lottery Association
4400 NW Urbandale Drive
Urbandale, IA 50322

Compliance Certification for: Multi-State Lottery Association (MUSL) RNG [REDACTED] using the [REDACTED] for the following games:

- Pick 3
- Pick 4
- Badger 5
- SuperCash! with SuperCash! Doubler
- Megabucks
- 5 Card Cash
- Special Draw (Raffle)

Reference Numbers:

BMM: [REDACTED]

Report Number: [REDACTED]

BMM CERTIFICATION TEST REPORT

1. STANDARD TESTED TO/RESULT

Technical Standard used for Compliance Evaluation	Test Result	
	Pass	Fail
GLI-11, Standards for Gaming Devices in Casinos v2.1 (August 25, 2011) Section 3.3 Random Number Generator (RNG) Requirements	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. PURPOSE

Multi-State Lottery Association has requested BMM Testlabs to perform an evaluation of the implementation of MUSL RNG [redacted] using the [redacted] for the following games: Pick 3, Pick 4, Badger 5, SuperCash! with SuperCash! Doubler, Megabucks, 5 Card Cash, and Special Draw (Raffle). In addition to the aforementioned Technical Standard, the evaluation for certification was conducted against the industry recognized standards for Random Number Generator (RNG) testing. The MUSL RNG [redacted] is designed to operate in conjunction with the [redacted]

3. SCOPE OF WORK

The certification of the MUSL RNG [redacted] using the [redacted] consists of a source code review and empirical statistical tests. The MUSL RNG [redacted] using the [redacted] implementation uses the [redacted] RNG algorithm. The [redacted] is used as a seeding method for the [redacted] RNG algorithm.

The MUSL RNG [redacted] using the [redacted] provides the RNG values for the games listed below as follows:

Draw Game	Picks	RNG Range
Pick 3	Three (3) numbers	Zero (0) to nine (9) with replacement
Pick 4	Four (4) numbers	Zero (0) to nine (9) with replacement
Badger 5	Five (5) numbers	One (1) to 31 without replacement
SuperCash!	Six (6) numbers	One (1) to 39 without replacement
SuperCash! Doubler	One (1) number	71 to 90
Megabucks	Six (6) numbers	One (1) to 49 without replacement
5 Card Cash	Five (5) numbers	One (1) to 52 without replacement
Special Draw (Raffle)	620 numbers	One (1) to 500,000 without replacement

BMM CERTIFICATION TEST REPORT

The source code review confirms the proper usage of the RNG algorithm including:

- The [REDACTED] RNG has a period [REDACTED].
- The RNG algorithm does generate numbers or values that are scaled accurately for the system design.
- The method of generating these numbers or values is unbiased and unpredictable.
- The [REDACTED] RNG itself is implemented into the system source code properly.
- The MUSL RNG [REDACTED] does not contain any malicious code that could significantly affect the outcome of the [REDACTED] RNG.
- The [REDACTED] is used as a seeding method for the [REDACTED] RNG algorithm.
- If the [REDACTED] is disconnected from the MUSL RNG [REDACTED], an alternate method of seeding the [REDACTED] RNG will not be used.
- The MUSL RNG [REDACTED] does not rely on the operating system of the computer it is executing on for randomness.

The industry recognized standard for statistical testing includes, but is not limited to: Chi-squared, Simple Number Frequency, Correlation tests, Run, Gap, Birthday Spacing, Coupon Collector, and Die Hard suite of tests. BMM also tested samples for generation and use without replacement. These tests are intended to verify the statistical properties of the RNG output and demonstrated the correct use of the RNG. Refer to Appendix 2 for a detailed explanation of the tests performed.

4. CERTIFICATION RESULTS

The source code review of the RNG and empirical statistical RNG testing MUSL RNG [REDACTED] using the [REDACTED] confirms:

- BMM Testlabs confirms the randomness of the MUSL RNG [REDACTED] and the suitability for its use of generating outcomes for the aforementioned games.
- The RNG itself is implemented into the system source code properly.
- The RNG does not contain any malicious code that could significantly affect the outcome of the RNG.
- There are no secondary decisions within the overall MUSL RNG [REDACTED] using the [REDACTED].
- The RNG algorithm is capable of generating numbers or values that are scaled accurately for the Pick 3, Pick 4, Badger 5, SuperCash! with SuperCash! Doubler, Megabucks, 5 Card Cash, and Special Draw (Raffle) games.
- The method of generating these numbers or values is unbiased and unpredictable.
- If the [REDACTED] hardware RNG is disconnected from the MUSL RNG [REDACTED], an alternate method of seeding the [REDACTED] RNG will not be used.
- The MUSL RNG [REDACTED] does not rely on the operating system of the computer it is executing on for randomness.
- The overall results of the statistical tests are probabilities that are expected to be uniformly distributed between zero (0) and one (1). Refer to Appendix 3, which contains a chart showing the distribution of the overall test results as well as specific charts for the Frequency, Gap, and Coupon tests.

BMM CERTIFICATION TEST REPORT

5. CERTIFICATION DETAILS

5.1. Software Version Details:

The following table details the relevant information for the MUSL RNG [redacted] using the [redacted] that has been certified as compliant to the aforementioned jurisdictional Technical Standard and industry recognized standards for RNG testing:

File Name	SHA-1 Signature	Validation Program Used
[redacted]	[redacted]	[redacted]

5.2. Software Signature Verification Information:

Signature Verification Application:

- (1) The SHA-1 signatures were calculated and verified using the BMM Signatures proprietary verification tool, which has been calibrated in accordance with ISO/IEC 17025 sections 5.5.2, 5.5.a, 5.5.c, and 5.5.8; as well as ISO/IEC 17020 sections 9.4, 9.6.b, 9.13.a, and 9.15.

(2) [redacted]

5.3. Hardware Requirements:

The following table details the relevant information for the hardware that has been certified as compliant to the aforementioned jurisdictional Technical Standard and industry recognized standards for RNG testing:

Hardware	Method of Connection
[redacted]	[redacted]

*This certification report does not preclude the use of other properly operating [redacted]

BMM CERTIFICATION TEST REPORT

6. ASSOCIATED SOFTWARE

The following associated software was used for the certification of the MUSL RNG [REDACTED] with the [REDACTED] games using the [REDACTED]

File Name	SHA-1 Signature	Validation Program Used
[REDACTED]	[REDACTED]	[REDACTED]

7. ADDITIONAL NOTES

- The hardware mentioned in this report must be used with the MUSL RNG [REDACTED] using the [REDACTED] software by design.
- Appendix 1 Table of RNG Statistical Tests Results gives the results of the different RNG tests.
- Appendix 2 Definition of Statistical Tests gives the details of tests performed during the RNG evaluation.
- Appendix 3 Overall RNG Statistical Tests, Frequency, GAP, Coupon Test Results contains a chart showing the distribution of test results.
- Appendix 4 Overall RNG Statistical Test Results contains a chart showing the distribution of test results for each of the aforementioned games.

BMM CERTIFICATION TEST REPORT

8. TERMS AND CONDITIONS

BMM Testlabs (BMM) has conducted a level of testing of the gaming product which has historically been adequate for a submission of this type. However, inherent in testing in a laboratory environment are the unavoidable limitations of it not being possible to verify the effects of all possible configurations and environments that occur in actual gaming venues.

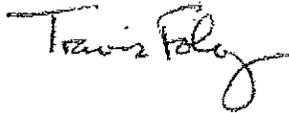
This certification report is for use by the named jurisdiction and only certifies the gaming product described in the report subject to any conditions or limitations set forth therein.

The manufacturer named in the report is solely responsible for possession of the appropriate license to sell, lease, service or provide gaming supplies or gaming related services in the jurisdiction for which this product was tested. It is the responsibility of the manufacturer and operators to ensure that the gaming product certified in this report is maintained and operated correctly without defects and safely within the venue environment.

This report shall not be reproduced, except in full, without the written approval of BMM. Upon request by an authorized party, BMM will send this recommendation for certification report via email as directed. BMM takes the precautionary measures to secure the "PDF" document but BMM does not send the email via any encrypted methodology if requested by an authorized party.

Please feel free to contact BMM Testlabs if you have any questions in regards to this certification report.

Yours sincerely,



Travis Foley
Executive Vice President, Operations
BMM Testlabs

T/ ic, jl

G/ jl

BMM CERTIFICATION TEST REPORT

Appendix 1:

Table of RNG Statistical Tests Results

Random Number Statistical Tests	Test Result			
	Pass	Fail	Not Tested	N/A
Chi-Square Analysis	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Frequency Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Pair Correlation Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Triples Correlation Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Quads Correlation Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Runs Up Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Runs Down Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Serial Correlation Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Gap Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Coupon Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Birthday Spacing Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overlapping 5-Permutation Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Binary Rank Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bitstream Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OPSO (Overlapping Pairs Sparse Occupancy) Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
OQSO (Overlapping-Quadruples-Sparse-Occupancy) Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DNA Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Count-The-1's Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Parking Lot Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Minimum Distance Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3D Spheres Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Squeeze Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Overlapping Sums Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Craps Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kolmogorov-Smirnov (KS) Test	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

BMM CERTIFICATION TEST REPORT

Appendix 2:

Definition of Statistical Tests

The Chi-Square statistical analysis verifies the distribution of the sum of the squared deviations.

The Frequency statistical analysis consists of the categorization of data. In an RNG sense, it is the number of times a specific number occurs over the entire sample of data.

The Pair Correlation statistical test analyzes the relationship between two (2) numbers. In an RNG sense, the first two (2) numbers produced by the RNG are tested to see if there is a relationship between the two. Then the second number and the third are compared. And so on.

The Triples Correlation statistical test analyzes the relationship between three (3) numbers. In an RNG sense, the first three (3) numbers produced by the RNG are tested to see if there is a relationship between the three. Then the second, third, and fourth numbers are compared. And so on.

The Quads Correlation statistical test analyzes the relationship between four (4) numbers. In an RNG sense, the first four (4) numbers produced by the RNG are tested to see if there is a relationship between the four. Then the second, third, fourth, and fifth numbers are compared. And so on.

The Runs Up statistical analysis looks for trends in the sequence of numbers produced by the RNG. For example, if the first numbers are 0, 6, 9, 11, 12, and 10, then there is a run up of five (5) numbers and the count starts over again, the total number of runs-up are then compared to the total samples produced.

The Runs Down statistical analysis looks for trends in the sequence of numbers produced by the RNG in the opposite directions of the Runs Up test.

The Gap Test counts the number of gaps between numbers produced by the RNG and then compares it to the total sample size.

The Birthday Spacing Test counts how many times there are any equal spacing in groups of numbers.

The Coupon Test counts how many numbers it takes to complete a set. The RNG output is analyzed for this type of trend.

The Serial Correlation Test looks for repeating patterns within the RNG output.

The Overlapping 5-Permutation Test divides the input data into a stream of bytes, and it considers five (5) bytes at a time. It compares the ordering of the five (5) numbers. There are 120 (5!) possible arrangements of ordering of these and each ordering should be equally probable.

The Binary Rank Test is for different sizes of matrices of the RNG output. Depending on the matrix size, a 32 bit random integer from the RNG output creates the matrix. The ranks of the different matrices are determined. A chi-square analysis is performed on the counts of the ranks. This is performed with 32x32, 31x31, and 6x8 matrices.

The Bitstream Test looks at the files as a stream of bits. When broken into 20 bit overlapping words, the test counts the number of missing 20 bit words.

The OPSO (Overlapping Pairs Sparse Occupancy) Test looks at the RNG output files in a sense of two (2) letter words from an alphabet of 1,024 letters and looks for the missing letters.

BMM CERTIFICATION TEST REPORT

Definition of Statistical Tests (Appendix 2 continued)

The OQSO (Overlapping-Quadruples-Sparse-Occupancy) Test looks at the RNG output files in a sense of four (4) letter words from an alphabet of 32 letters. The test then looks for the missing letters.

The DNA Test considers an alphabet of four (4) letters C, G, A, and T. Two (2) designated bits determine these letters in the sequence from the RNG output files. It considers ten (10) letter words and looks for the missing words similar to the OPSO and OQSO tests.

The Count-The-1's Test looks at the files as a stream of bytes. Each byte may contain a number from zero (0) to eight (8) ones, with given probabilities. When these bytes are overlapping they can be put into five (5) letter words where each letter could be A, B, C, D or E. The test then verifies the frequencies of each word. This test is then repeated on designated bytes.

The Parking Lot Test considers a square with a side of 100. Then the file is read and each value is attempted to "park" within the square. The number of success verses attempts is then analyzed.

The Minimum Distance Test is performed one 100 times. From the RNG output file 8,000 random points in a square 10,000x10,000 are chosen. The minimum distance between the pairs of points is analyzed.

The 3D Spheres Test picks 4,000 random points from the RNG output file within a cube 1,000x1,000x1,000. At each point, a sphere is mapped to be large enough to reach the next point. The radius of each sphere is cubed and should be within the mean of 30.

The Squeeze Test finds out how many iterations of k are required to reduce k to one (1). The starting value of k equals 231^{-1} . The iteration process uses the formula $k=k*uni()+1$ where $uni()$ is a sequence of random integers from the RNG output file. The number of iterations is found to reduce k to one (1) and then the reduction over again 100,000 times with a different sequence of random integers from the RNG output file. The number of iterations is then analyzed with a chi-square test for cell frequencies.

The Overlapping Sums Test uses a series of integers from the RNG output file and then they are made into floating point numbers over a range of (0, 1). Then they are summed in an overlapping series of 100. The sums are normalized with a specified covariance matrix. These values are then converted to uniform variables for the Kolmogorov-Smirnov (KS) test.

The Craps Test uses 32 bit values from the RNG output files as the results of 200,000 games of craps. The number of wins should have a normal with a mean of $200,000p$ and variance of $200,000(1-p)$ where $p = 244/495$. The throws necessary to complete the game can vary from one (1) to infinity, but counts for all throws greater than 21 are lumped with 21. A chi-square test is conducted over the number of throws frequency counts.

The Kolmogorov-Smirnov (KS) Test determines if two (2) datasets differ significantly in the form of minimum distance estimation.

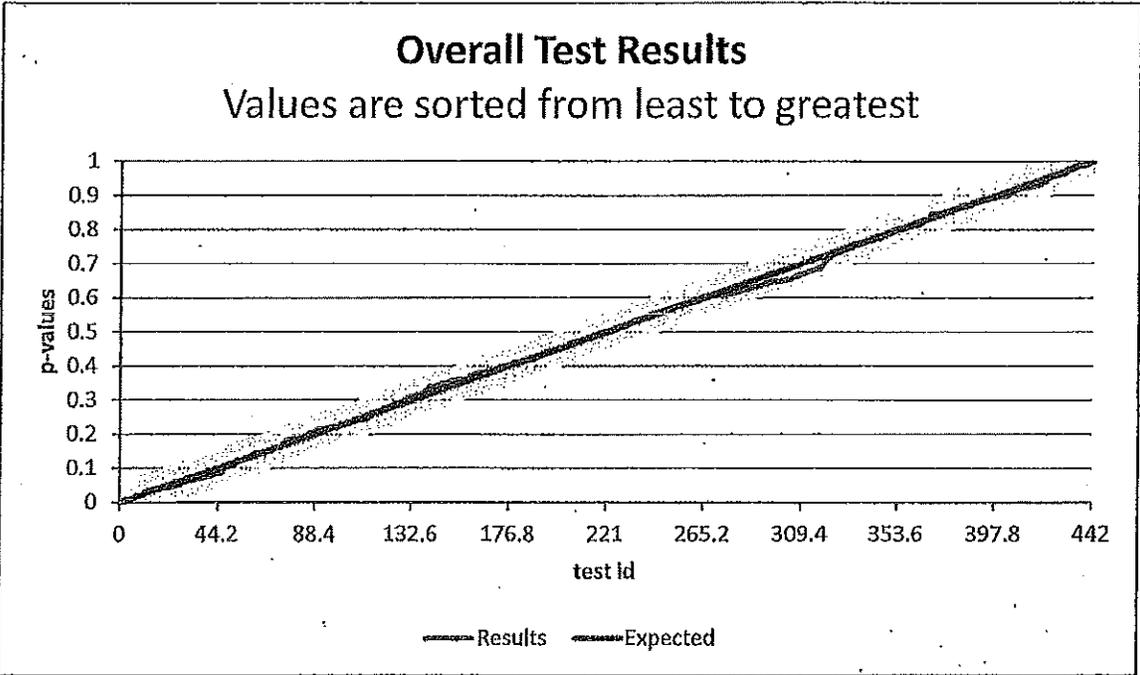
BMM CERTIFICATION TEST REPORT

Appendix 3:

Overall RNG Statistical Tests, Frequency, GAP, Coupon Test Results

The results of the Statistical tests are probabilities that are expected to be uniformly distributed between zero (0) and one (1). This chart shows those test results plotted against an expected result indicator of perfect distribution from zero (0) to one (1) with error bars for a fixed 0.05 error shown. This shows that the RNG stays within the expected outcome and produces statistically strong random numbers.

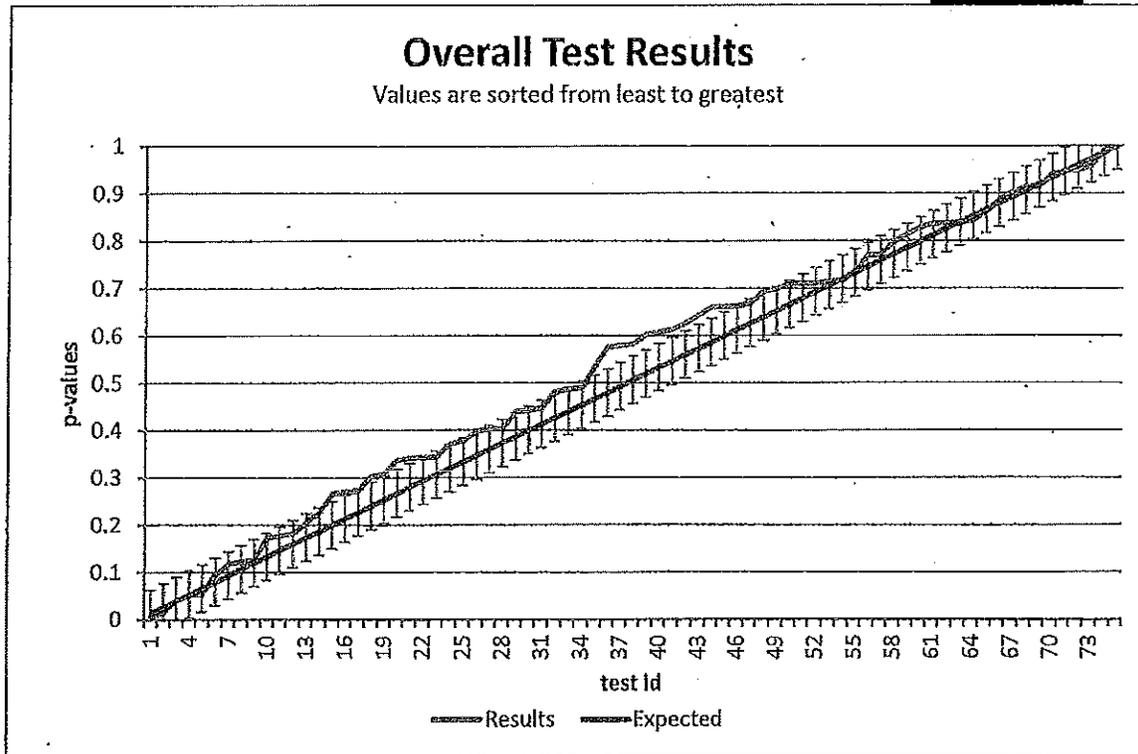
Results for [redacted] RNG:



BMM CERTIFICATION TEST REPORT

Appendix 3 Continued:

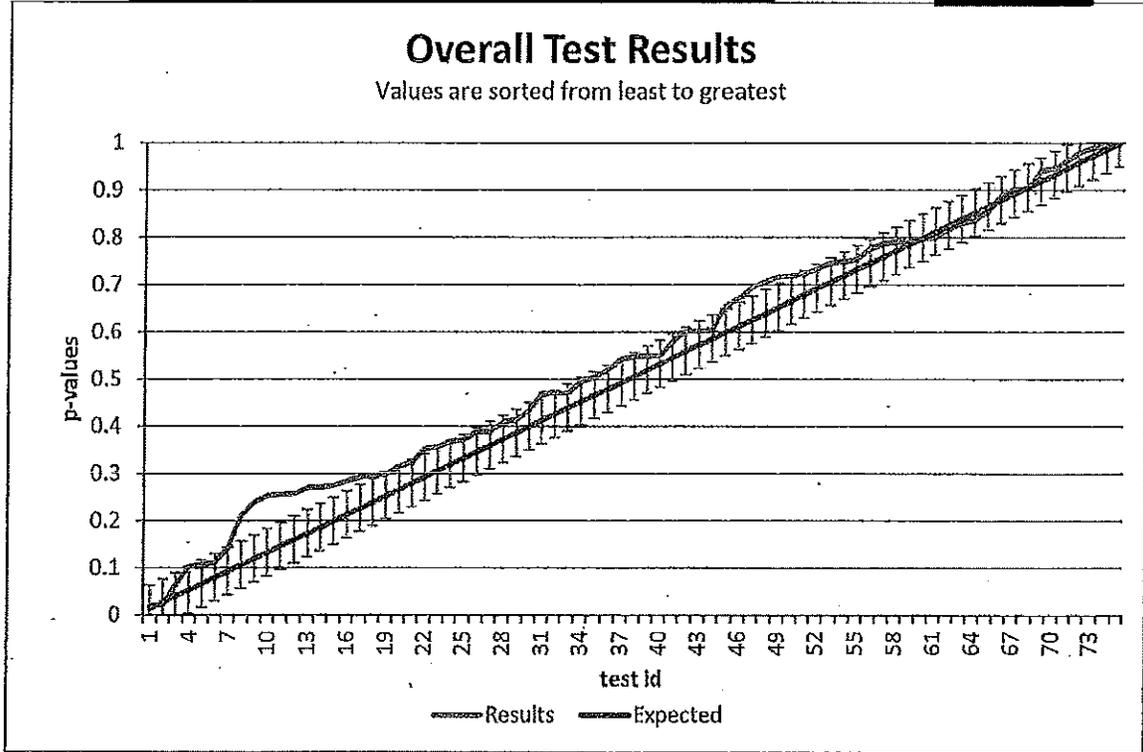
Results for [REDACTED] Serial Number [REDACTED]



BMM CERTIFICATION TEST REPORT

Appendix 3 Continued:

Results for [REDACTED] Serial Number [REDACTED]

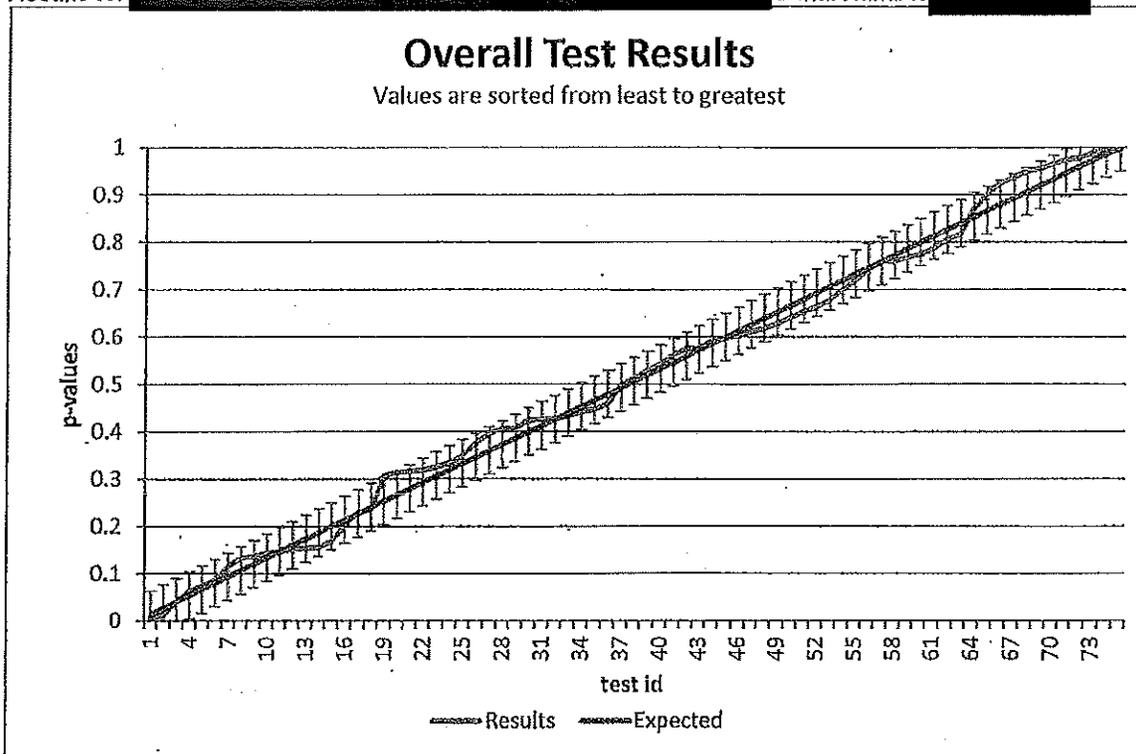


BMM CERTIFICATION TEST REPORT

Appendix 3 Continued:

Results for [REDACTED]

Serial Number [REDACTED]

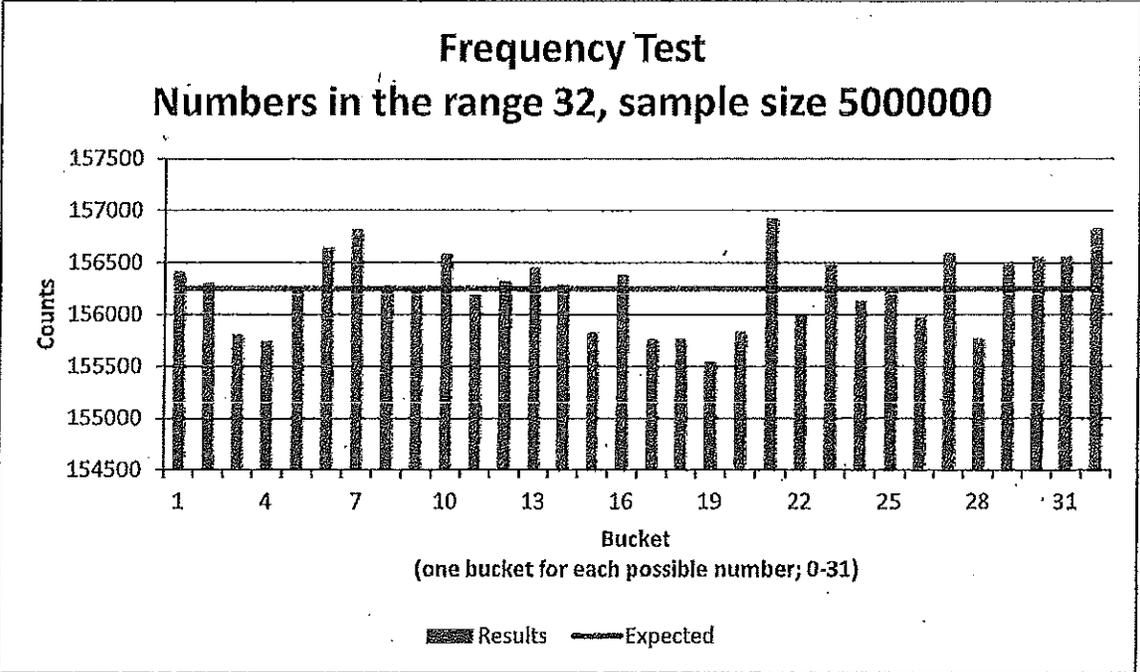


BMM CERTIFICATION TEST REPORT

Appendix 3 Continued (Frequency Test):

The Frequency test chart for the range of numbers from one (1) to 32 with 5,000,000 samples displays the possible total count of each number and the actual total count of each number.

Results for [redacted] RNG:

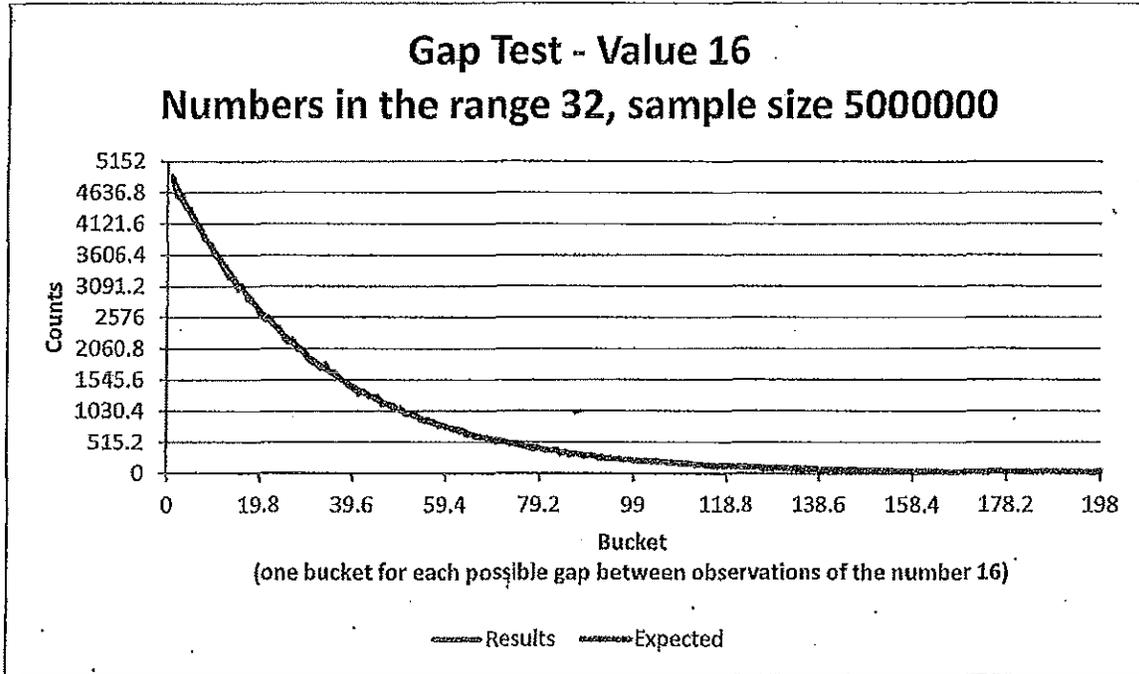


BMM CERTIFICATION TEST REPORT

Appendix 3 Continued (Gap Test):

The Gap test chart for the number 16 for 5,000,000 RNG samples generated with a range between zero (0) and 32. This test measures the expected distance between each occurrence of the number 16 and the actual distance between each occurrence over 5,000,000 RNG samples.

Results for [redacted] RNG:

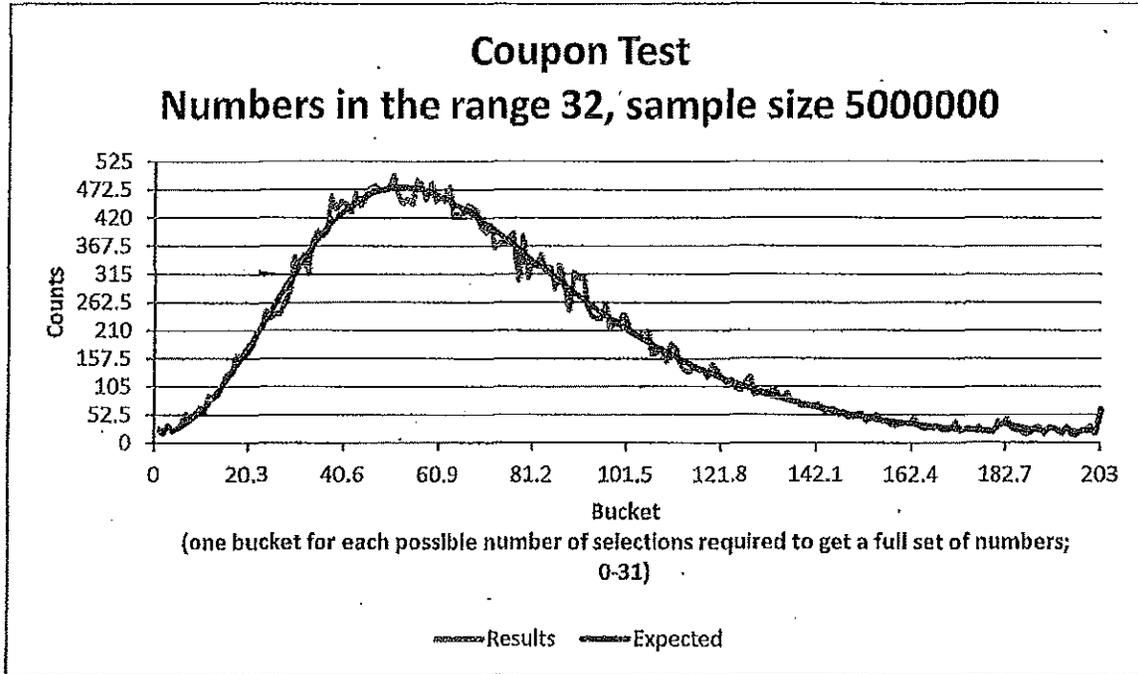


BMM CERTIFICATION TEST REPORT

Appendix 3 Continued (Coupon Test):

The Coupon test chart is for the range of numbers from one (1) to 32 with 5,000,000 samples displays the possible number of selections required for a full set of numbers of one (1) though 32.

Results for ████ RNG:



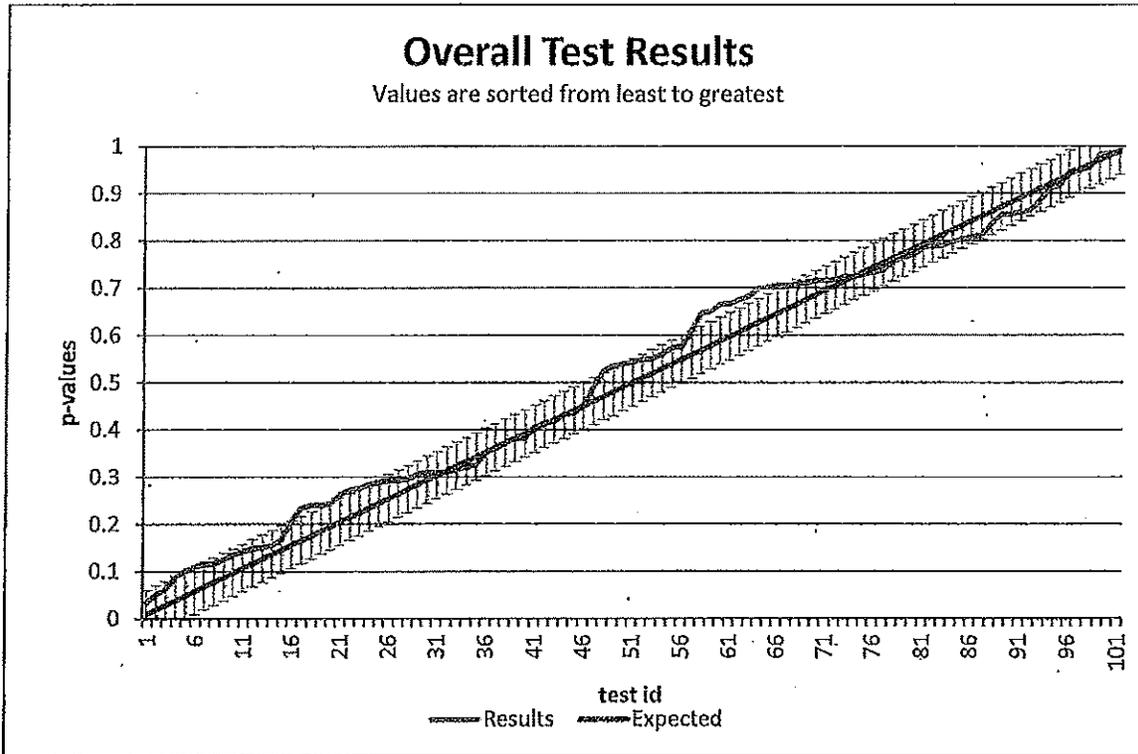
BMM CERTIFICATION TEST REPORT

Appendix 4:

Overall RNG Statistical Test Results

The results of the Statistical tests are probabilities that are expected to be uniformly distributed between zero (0) and one (1). This chart shows those test results plotted against an expected result indicator of perfect distribution from zero (0) to one (1) with error bars for a fixed 0.05 error shown. This shows that the RNG stays within the expected outcome and produces statistically strong random numbers.

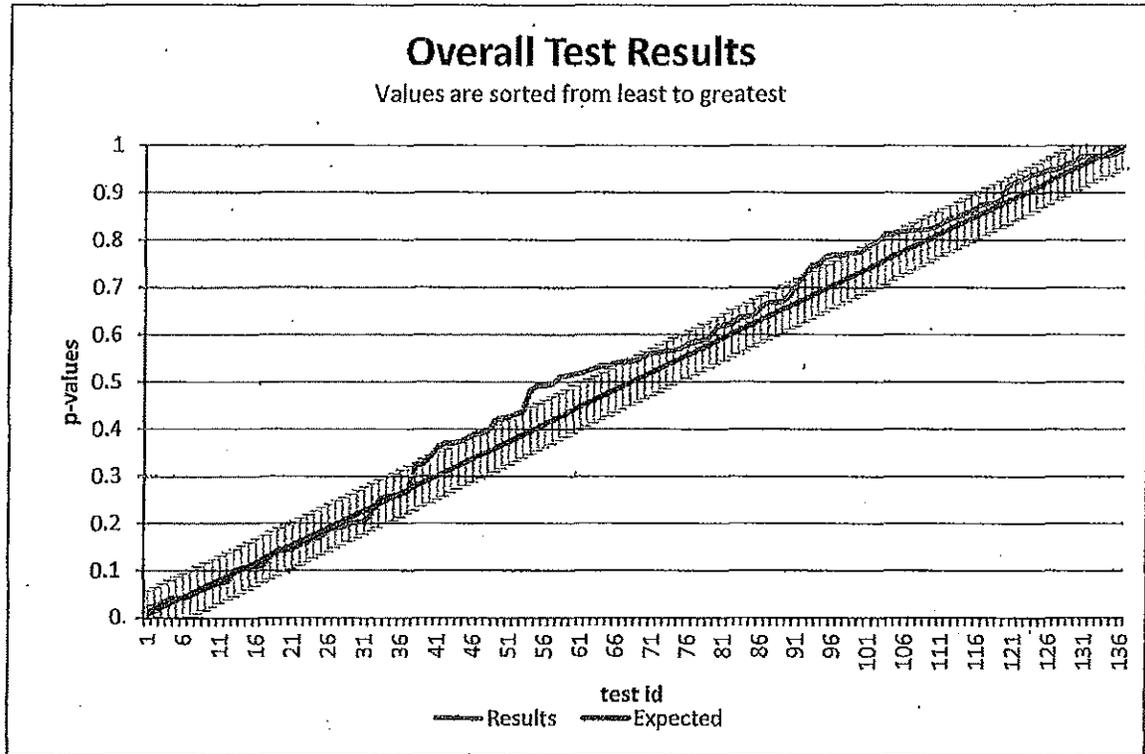
Results for Pick 3 (Sample Size 100,000):



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

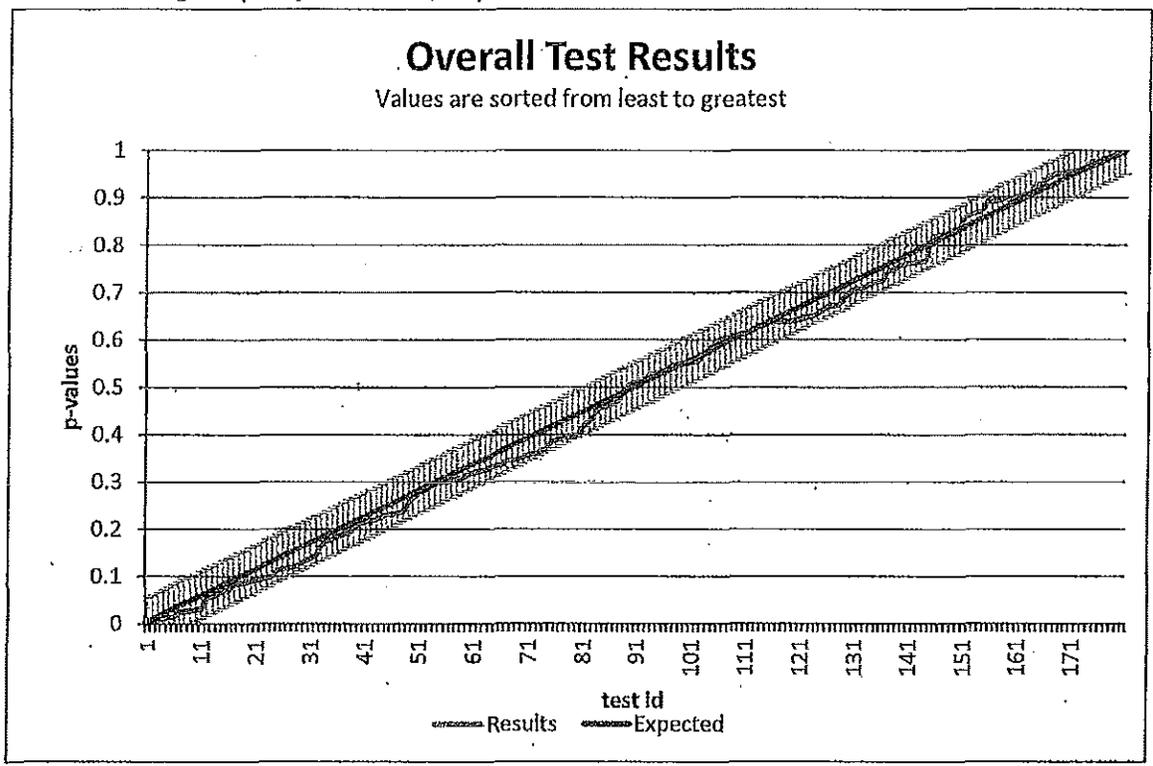
Results for Pick 4 (Sample Size 100,000):



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

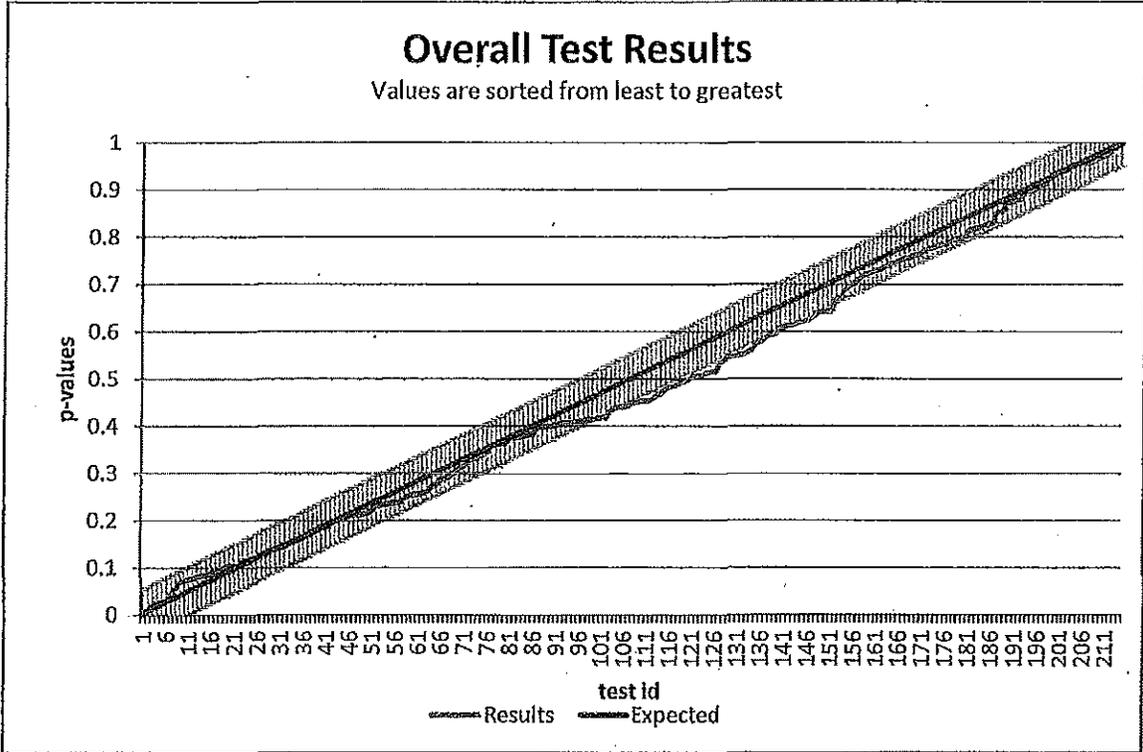
Results for Badger 5 (Sample Size 100,000):



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

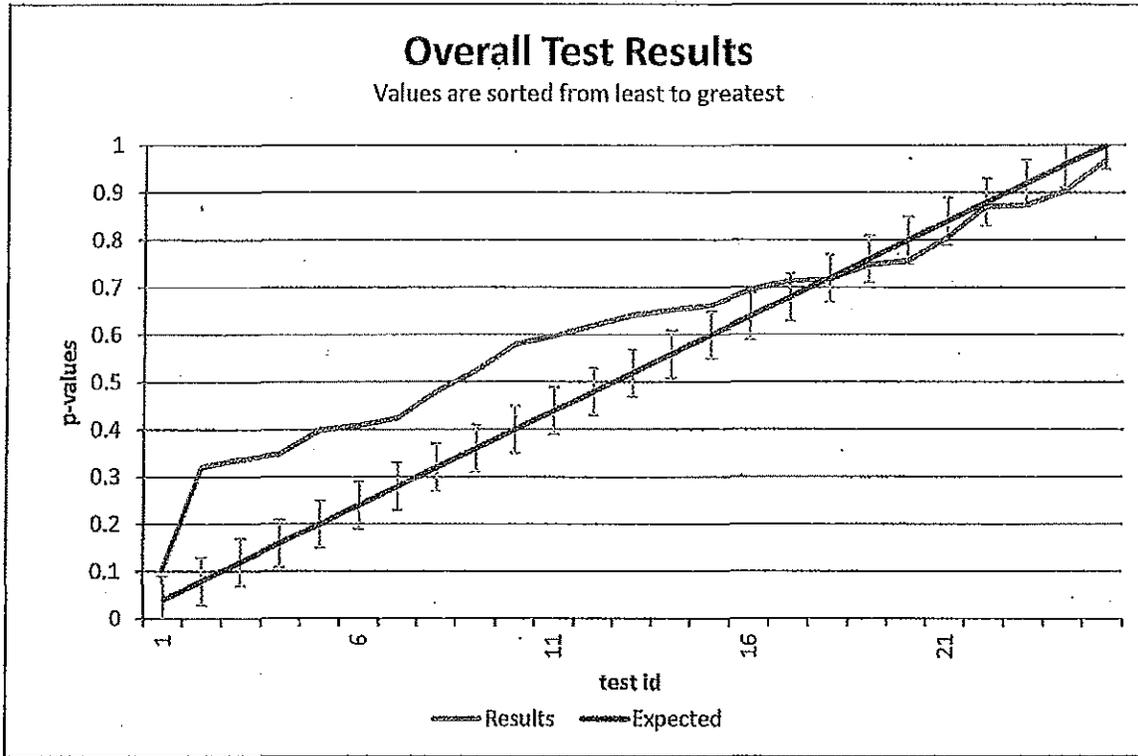
Results for SuperCash! (Sample Size 100,000)::



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

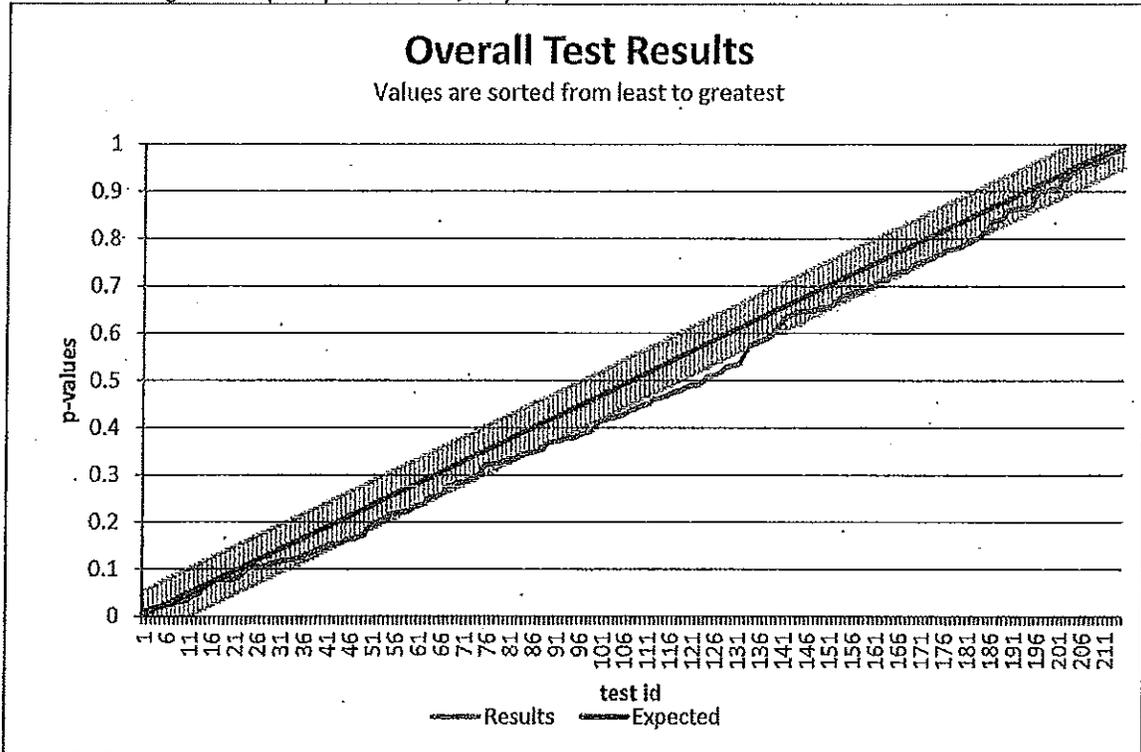
Results for SuperCash! Doubler (Sample Size 100,000):



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

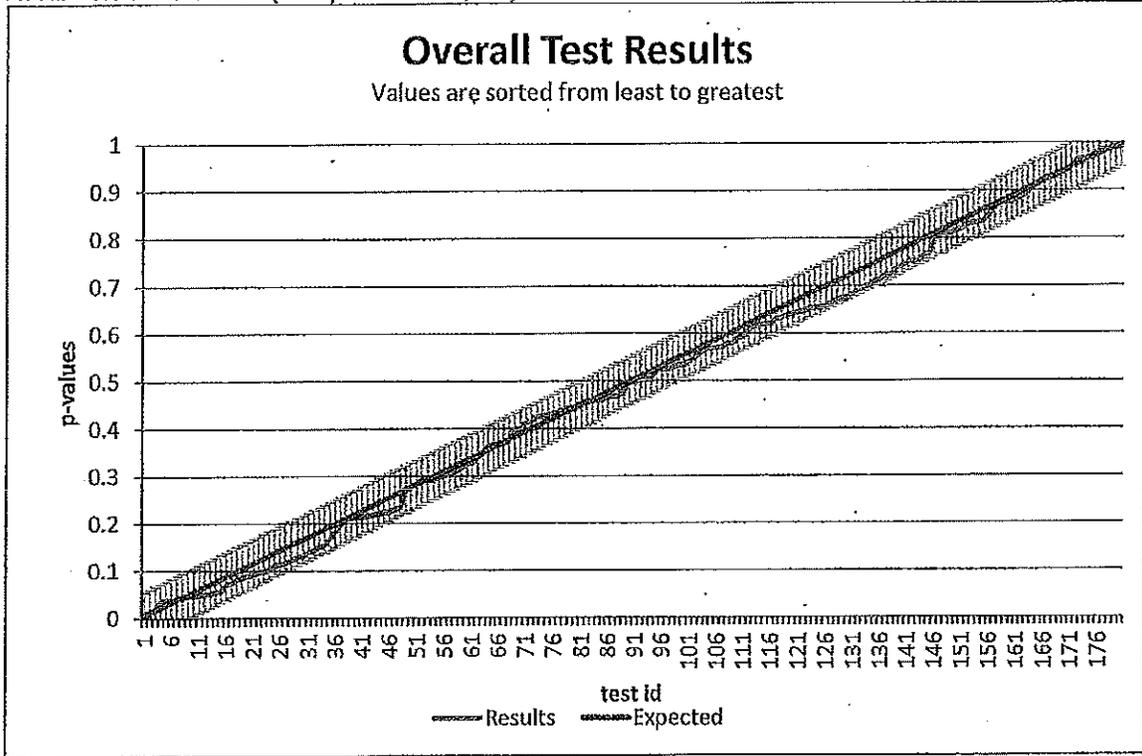
Results for MegaBucks (Sample Size 100,000):



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

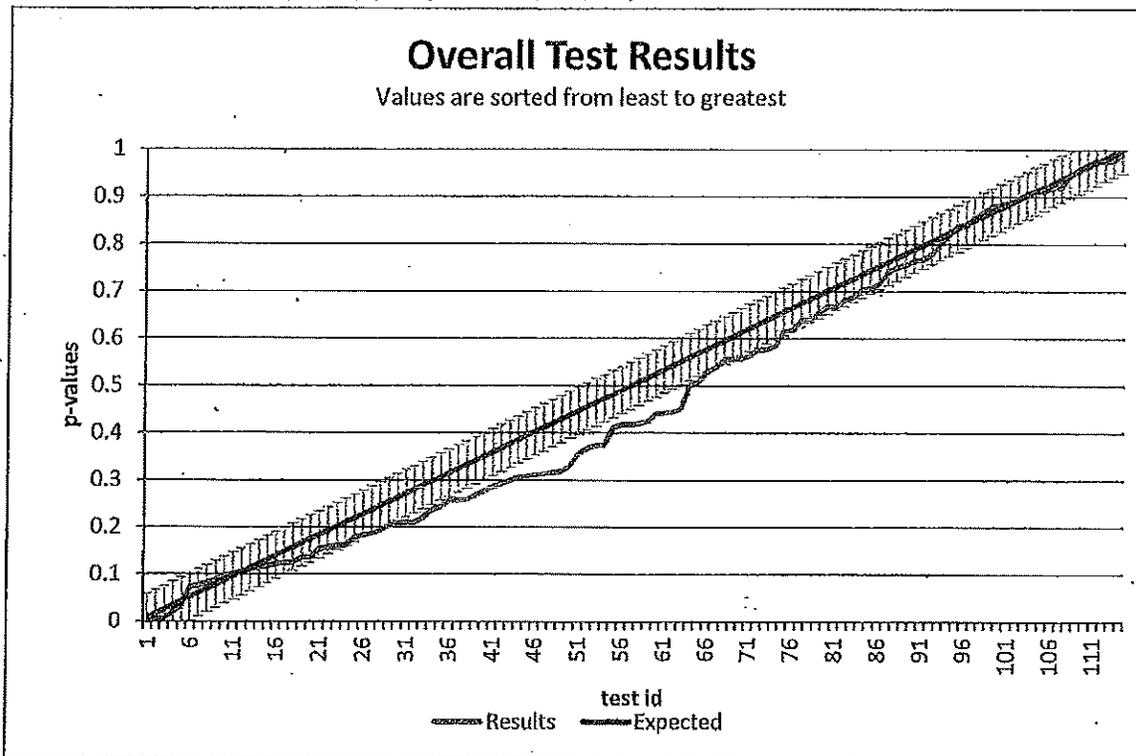
Results for 5 Card Cash (Sample Size 100,000):



BMM CERTIFICATION TEST REPORT

Appendix 4 Continued:

Results for Special Draw (Raffle) (Sample Size 6,000,000):



CONFIDENTIAL



Corporate Headquarters
17185 W. Glendale Dr.
New Berlin, WI 53151

CONFIDENTIAL REPORT OF FINDINGS

REPORT DATE: June 11, 2015

CASE NUMBER:

I. EXECUTIVE SUMMARY

A. Background

In accordance with the scope of work provided by [redacted], Digital Intelligence ("DI") examined three automated drawing machines utilized by the Wisconsin Lottery. Specifically, DI examined the systems to identify unusual, questionable or suspect activity or files on any of the computers.

B. Conclusions

After comprehensive evaluation and testing as detailed in this report, our findings confirm the stability of the systems and the absence of any unusual, questionable or suspect activity on the RNG computer systems in use by the Wisconsin Lottery. Furthermore, the examinations and subsequent analysis revealed no indication of malicious or anomalous files on the systems and no malicious or anomalous activity arising out of the execution of the RNG application,

C. Disposition of Digital Files

CONFIDENTIAL

II. DISCUSSION

A. Overview of Process and Assumptions

When analyzing a system where there are no known issues or incidents that call in to question the system's integrity, it is important to utilize a comprehensive, methodical and repeatable process that seeks to identify anomalies from a known standard. To this end, DI utilized the following process:

B. COLLECTION

On May 5, 2015, DI Sr. Forensic Examiner, received access to the following computers utilized by the Wisconsin Lottery:

CONFIDENTIAL

C. SYSTEM ANALYSIS

The forensic copies of the computer systems were examined for installed files, accounts, hardware, and activity utilizing

The registry is a set of files that comprise a database of configurations for the system. These configurations include hardware, software and user settings. The Windows Registry from each of the systems was examined for the following:

1. Operating system information;
2. User profile data;
3. Network connections;
4. Installed programs that are configured to run;
5. Installed programs that are configured to run a single time; and
6. Connected USB storage devices.

1. *Operating System Analysis*

Figure C-1 contains a summary of Operating System information for each of the three systems.

All systems have the same installation date and time of _____ at _____. Furthermore, all systems are running Windows 7, _____. These two factors are consistent with the systems being installed from a standard image, _____. Assuming the standard computer image used by MUSL is consistent with these creation dates, no suspicious or malicious activity can be concluded based on the operating system artifacts.

2. *User Accounts*

CONFIDENTIAL

Figure C-2.1 – User Account Last Login

Figure C-2.2 – User Account Last Password Change

The discrete set of user accounts and login information is consistent with the use of the systems . No deleted accounts or unusual account activity are apparent based on the analysis of the User Account information.

CONFIDENTIAL

3. Network Connections

Figure C-3 contains a summary of Network connection records.

: This appears to be consistent with the installation and/or configuration of the systems. No other unwarranted network connection information was detected.

4. Programs Configured to RUN on startup

During the Windows boot process it is possible to have programs that are executed automatically. This can be a source of malicious activity as the unidentified programs are executed without user intervention.

CONFIDENTIAL

The programs listed above were consistent across all three systems and no issues were detected with any of the programs. The purpose of these files is as follows:

Nothing of apparent concern was noted in the examination of the Registry key listed below or in the analysis of the files listed.

5. *Programs Configured to Run Once*

Malware programs are often detected in the Registry under . This key was empty on all three systems.

6. *USB Connected Devices*

CONFIDENTIAL

CONFIDENTIAL

D. File Comparison

CONFIDENTIAL

E. DLL and EXE File Identification

Most malware comes in the form of an executable process and is commonly found in .DLL files, Dynamic Link Libraries, and .EXE files, which are executable programs. The .DLL files and the .EXE files identified below in the Memory Analysis section as code that were actually run on the systems were compared to the Hash libraries. All but approximately 40 of the files were known non-threatening programs to the NIST library (see Exhibit E). The remaining files were manually reviewed and found also be known non-threatening programs.

The only programs that were not verified as known were [redacted] and [redacted]. The hash value calculated for the [redacted] program is [redacted]. The same value was calculated for all copies of the [redacted] program from all three of the computer systems. The resultant conclusion is that there are no differences in the copies of the [redacted] program. The [redacted] program also generated the same MD5 hash value across all three computers, also indicating that no difference exists in this program among the computers. The MD5 hash value for the [redacted] program is [redacted]. Further examination of these files is included in the Memory Analysis section of this report.

In this case, we have come to the conclusion that no foreign executable code is being run in association with the [redacted] program or the [redacted] program.

F. Deleted Files

Files marked as deleted on each of the systems were reviewed. When a file on an NTFS volume (such as that utilized on the computers in this case) is deleted, the contents are not immediately removed. The NTFS file system uses a special database called the Master File Table (MFT) to track all files and stores the name of the files together with the location on the drive where the contents are stored. When a file is deleted, the database record for that file is marked to indicate that it is no longer in use. This means that the record containing the file's name can be reused (overwritten) and the storage location of the contents can be reused (overwritten). If the record and storage location have not been reused, then the file is typically recoverable. Once a record or the storage location are reused, the original data, filename or content, cannot be recovered. However, the database record will not necessarily be reused at the same time the storage area is reused. In some instances the file name is available but the

CONFIDENTIAL

contents are not; in other instances the contents are available, but the file name is not. For purposes of this examination, the available filenames from files marked as deleted were examined.

Examination of the deleted files does not indicate any unusual activity. Deleted files are consistent with normal Microsoft Windows usage.

The Windows operating system routinely creates and deletes files most notably during updates and installation periods. It is expected to find thousands of deleted files over the course of several years of operation. If a malware program is creating and deleting files, this would be reflected in recent activity. No such activity was noted in the examination of the listing of deleted files in Exhibit F.

G. Anti-Virus Scans

The forensic copies created from each system were mounted and scanned for malware . No malware was detected in the scan.

H. Virtual Machines

Using a program named , bootable instances of the three computers were created from the forensic copies that were made. The purpose of the virtual instances is to allow testing of a "live" system without actually using and altering the original computer setup. These virtual machines were used for the memory analysis described below. The program creates compatible images that allow the copy to be booted in a virtual environment just as the physical computer is booted. is an industry standard virtual computing software environment. The program bypasses the need the for login credentials, so each of the accounts on the computers can be tested.

I. Memory Analysis

For the purpose of determining whether malware or other unauthorized code may be present on the systems, we analyzed the active memory of all machines. This process allows us to identify all programs and processes that are active and running when the machine is in operation.

In addition to the RAM memory captures identified in Figure B-3, above, nine additional RAM memory captures were collected from the three computers. To obtain these memory captures, DI logged into each virtual machine with each User Account and captured the memory. Each virtual machine was accessed with three main User Accounts

Investigation of potential malicious code was performed, as follows:

1. All running and exited processes were identified by
2. The Dynamic Link Library loaded was identified for all processes
3. Identification of hidden and/or injected code from physical memory dumps was performed
4. Application Program Interface (API) hooks in user mode or kernel mode were identified and reviewed,
5. DLLs unlinked from one (or all) of the linked lists in were cross-referenced with the
6. The IDT (Interrupt Descriptor Table) was checked for rootkits hooking the IDT (IDT);
7. Rootkits that install a call gate so that user mode programs can call directly into kernel mode (GDT) were evaluated and assessed;
8. Examined each memory capture for the presence of important notification routines and kernel callbacks often used by Rootkits, anti-virus suites, dynamic analysis tools, and many components of the kernel that monitor and/or react to events, (DRIVEIP); and
9. Installed kernel timers (KTIMER) and any associated DPCs (Deferred Procedure Calls), (TIMERS) were reviewed.

CONFIDENTIAL

Exhibit I-1 contains a representative list of processes identified as active in memory on when logged in to the . None of the above processes are hidden which is common for malware. Based upon the foregoing analysis, no running or exited processes containing malware were found and no signs of malicious code were detected. Given the significance of the and programs, we conducted specific analysis of the DLLs loaded by these programs.

All but approximately 40 of the files were known non-threatening programs to the NIST library. The remaining files were manually reviewed and also found to be known, non-threatening programs.

III. CONCLUSIONS

After examiners performed the comprehensive examination and testing as set forth in the above mentioned protocol, no indication of malicious or anomalous files stored on any of the systems was found and no malicious or anomalous activity was found to have occurred.

DIFS, LLC d/b/a DIGITAL INTELLIGENCE

By:

CONFIDENTIAL

Exhibit E –
Page i of iii

CONFIDENTIAL

Exhibit E –
Page ii of iii

CONFIDENTIAL

Exhibit E –
Page iii of iii

CONFIDENTIAL

Exhibit F –
Page i of iii

CONFIDENTIAL

Exhibit F –
Page ii of iii

Exhibit F –
Page iii of iii

CONFIDENTIAL

Exhibit I-1 – Processes

Page i of i

CONFIDENTIAL

Exhibit I-2 –

Page i of ii

CONFIDENTIAL

Exhibit I-2 -
Page ii of ii

CONFIDENTIAL

Exhibit I-3 –

Page i of iii

Exhibit I-3 –

Page ii of iii

CONFIDENTIAL

Exhibit I-3 –
Page iii of iii

CONFIDENTIAL