|  |
| --- |
| <Logo> |
| **<Target>****Entropy Assessment and SP 800-90B Compliance Report**Document Version: v1.0Release Date: <Month dd, yyyy> |
| Prepared by:**<Company>**<Address><City, State ZIP><Country> |
| Prepared for:**<Customer>**Report ID <xx-xxxx> version YY |
|  |

**Change History**

|  |  |  |  |
| --- | --- | --- | --- |
| Report Version | Change Description | Date | Author |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distribution and Ownership**

<Include some explicit description of who owns the report and the IP contained within, to whom it can be distributed, and under what circumstances. Below, we have an example of such a thing.>

<Company> has granted <Customer> authorization to distribute unmodified copies of this report at <Customer>’s discretion. This report contains both <Customer>’s IP (the entropy source design and the portions of the analysis which are described as originating from <Customer> documentation) and <Company>’s IP (the portions of the analysis which are not described as originating from <Customer> documentation).

Table of Contents

[1 Introduction 5](#_Toc102385910)

[1.1 Report Applicability 5](#_Toc102385911)

[2 Entropy Source 7](#_Toc102385912)

[2.1 Noise Source(s) 7](#_Toc102385913)

[2.2 Health Tests 8](#_Toc102385914)

[2.3 Conditioning 9](#_Toc102385915)

[3 Noise Source Entropy Analysis 11](#_Toc102385916)

[3.1 Assumptions 11](#_Toc102385917)

[3.2 A Heuristic Entropy Estimate 11](#_Toc102385918)

[3.3 The Impact of Health Testing Requirements on 12](#_Toc102385919)

[4 Statistical Testing 13](#_Toc102385920)

[4.1 Raw Data Set Description 13](#_Toc102385921)

[4.2 Raw Data Testing, Formatting, and Extraction 13](#_Toc102385922)

[4.3 IID Testing 14](#_Toc102385923)

[4.4 Statistical Assessment of Raw Data 14](#_Toc102385924)

[4.4.1 The -Stabilized Result 14](#_Toc102385925)

[4.4.2 The Large Block Assessment 15](#_Toc102385926)

[4.4.3 The Overall Statistical Assessment 15](#_Toc102385927)

[4.4.4 Statistical Assessment Results 16](#_Toc102385928)

[4.5 Restart Testing 16](#_Toc102385929)

[5 Health Testing and Error Modes 17](#_Toc102385930)

[5.1 Assumptions 17](#_Toc102385931)

[5.2 Health Tests 17](#_Toc102385932)

[5.2.1 Health Test 1 17](#_Toc102385933)

[5.2.2 Health Test 2… 17](#_Toc102385934)

[5.3 Anticipated Failure Modes 18](#_Toc102385935)

[5.3.1 Failure Mode 1 18](#_Toc102385936)

[5.3.2 Failure Mode 2… 18](#_Toc102385937)

[5.4 Requirements for Developer-Defined Alternatives to the Continuous Health Tests 18](#_Toc102385938)

[5.4.1 SP 800-90B Section 4.5 Criterion (a) 18](#_Toc102385939)

[5.4.2 SP 800-90B Section 4.5 Criterion (b) 18](#_Toc102385940)

[6 Conditioning Analysis 19](#_Toc102385941)

[6.1 Assumptions 19](#_Toc102385942)

[6.2 Design-Based Conditioning Analysis for Non-Vetted Conditioning 19](#_Toc102385943)

[6.2.1 Non-Vetted Component 1 19](#_Toc102385944)

[6.2.2 Non-Vetted Component 2… 19](#_Toc102385945)

[6.3 SP 800-90B Conditioning Chain Analysis 19](#_Toc102385946)

[6.3.1 Conditioning Component 1 (Example: Vetted) 20](#_Toc102385947)

[6.3.2 Conditioning Component 2... (Example: Non-vetted) 20](#_Toc102385948)

[6.3.3 Conditioning Component 3… 21](#_Toc102385949)

[6.3.4 Conditioning Chain Results Summary 21](#_Toc102385950)

[7 Conclusion 22](#_Toc102385951)

[8 References 23](#_Toc102385952)

[Appendix A NIST Tool Output 24](#_Toc102385953)

[Smallest Raw Data Large Block Assessment 24](#_Toc102385954)

[Conditioned Data Assessment 24](#_Toc102385955)

[SP 800-90B Conditioning Calculation 24](#_Toc102385956)

[Restart Testing 24](#_Toc102385957)

[Appendix B SP 800-90B and FIPS 140 Requirement Mapping 25](#_Toc102385958)

[SP 800-90B “Shall” Requirements 25](#_Toc102385959)

[FIPS 140 IG Requirement Mapping 38](#_Toc102385960)

[8.1.1 IG 7.18 38](#_Toc102385961)

[IG 7.19 41](#_Toc102385962)

[Appendix C Modeling Calculations 47](#_Toc102385963)

[Appendix D Simulations 48](#_Toc102385964)

[Simulation Code 48](#_Toc102385965)

[Simulation Results 48](#_Toc102385966)

[Appendix E Glossary 49](#_Toc102385967)

[Notation Used 49](#_Toc102385968)

[Definitions 49](#_Toc102385969)

[Appendix F Data Gathering Procedures and Controls 50](#_Toc102385970)

[Data Gathering Procedures 50](#_Toc102385971)

[Raw Data Acquisition Procedure 50](#_Toc102385972)

[Restart Data Acquisition Procedure 50](#_Toc102385973)

[Conditioned Data Acquisition Procedure 50](#_Toc102385974)

[Vendor Attestation 50](#_Toc102385975)

# Introduction

[NIST SHALL] Requirement IDs to be addressed at a high level in this section (see Appendix B): 26, 27

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 7, 86

This document describes the design of the <Customer> <Target>, provides an analysis of the <Target> entropy, and describes how it satisfies the requirements of NIST SP 800-90B.

The entropy source (depicted in Figure 1) is composed of a few major sections, which map to the conceptual components contained within an SP 800-90B entropy source. The <Target> entropy source contains:

A primary noise source (and optionally one or more additional noise sources)

<Digitization>

Health tests

<A conditioning algorithm or a conditioning chain.>

<Describe the entropy source security boundary and its contents. This boundary must be well-defined and should be depicted in the entropy source figure.>

Figure 1. Entropy Source (from <Ref>)

<High level description of the entropy source. If an IID claim is going to be made, identify that here and provide a brief summary of why the noise source can be thought of as IID.>

## Report Applicability

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 25

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B):34, 58

This assessment was conducted using data and parameters measured in the evaluated version and configurations described within this report. The evaluated version is shown in Table 1 and all entropy-relevant parameters (i.e., operating conditions) must be set as specified in Table 2.

Table 1. Evaluated Version

|  |  |
| --- | --- |
| Identifier | Version |
| Part Number (if applicable) | <Part number> |
| Hardware Revision (if applicable) | <Revision> |
| Firmware Version (if applicable) | <Version> |
| Software Version (if applicable) | <Version and link to code if open source> |

Table 2. Entropy-Relevant Parameters

|  |  |  |
| --- | --- | --- |
| Parameter | Value | Description |
| Temperature | <value> | <Description> |
| Voltage | <value> | <Description> |
| Clock speed | <value> | <Description> |
| Compiler options | <value> | <Description> |
| <configuration parameter 1> | <value> | <Description> |
| <configuration parameter 2> | <value> | <Description> |

**The findings of this evaluation are specific to the particular part/version and entropy-relevant parameters that are documented and do not apply more broadly. If the entropy-relevant parameters are different than those described in this report, then additional modeling and statistical testing are required. Any part/version or configuration other than that described above is not covered by this report.**

# Entropy Source

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B): 22.

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 24, 86

The entropy source (depicted in Figure 1) is composed of a few major sections, which are described in detail within this section:

The primary noise source

Digitization

<Any additional noise sources>

The entropy estimator (health tests)

<The conditioning>

<Describe the high-level interactions between the noise source(s), health tests, and conditioning.>

## Noise Source(s)

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 28, 30, 31, 39, 40, 42, 44

[NIST SHALL] Requirement IDs that may be partially addressed in this section (see Appendix B): 7, 33, 34, 38, 41, 43, 95, 96, 97, 98, 99, 100, 115, 116

<Detailed description of the noise source and its operation. This does not generally include an entropy level argument. This includes how the noise source works, where the unpredictability comes from, and rationale for acceptable entropy output. References to existing research and literature should be given and included in Section 8.>

<Describe the digitization process. Note that this includes combining outputs of noise source copies.>

<Describe the mechanism/interface used to generate raw data directly from the noise source and whether it is available during normal operating mode or only in a test environment. If the mechanism is available during normal operating mode, describe how its output cannot be provided to a conditioning component or used as eventual normal entropy source output. Declare (this value will be justified later in Sections 3.2 and 3.3). If the mechanism is available only in a test environment, explain how use of this test environment will not alter the behavior of the entropy source (in comparison to normal operating mode).>

The high-level design of this noise source is shown in Figure 2. <Sometimes additional figures are useful, particularly to describe what high-level portions of this design do.>

Figure 2. Noise Source (from <Ref>)

<Describe the relevant design parameters that ultimately are used and provide values (generally in tables).>

<The noise source produces raw data whose format is… The description must include the length (in bits) of the fixed-length bitstrings used to represent the raw symbols, the output space, and a list (or range) of all possible outputs.>

<Indicate if the noise source produces non-IID data or IID data.>

<If an IID claim is being made, this argument is described in detail here.>

<If additional noise source outputs to increase security are used, this must be described. (Note: Additional noise sources cannot be credited as providing entropy, and (if conditioning is present) the additional noise source and primary noise source outputs must be combined in a vetted conditioning component.)>

## Health Tests

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 66, 68, 69, 74

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 61, 62, 63, 64, 67, 71, 72, 73, 75, 76, 90, 118, 119, 121

<A detailed description of each of the health tests goes here. Describe any parameters that affect each health test (e.g., the type of data used by each health test, the targeted false reject rate, , the APT’s window size, W, and the APT’s and RCT’s cutoff parameters, C). Describe which health tests are applied to the raw noise samples (i.e., before any conditioning is done) if there are any additional health tests performed on conditioned data.

<Classify each included health test (start-up health test / continuous health test / on demand health test).>

<Include a description of start-up behavior.>

<Include a description of continuous behavior. Is it the Approved test or a developer-defined test?>

<Include a description of on-demand behavior.>

<Include a high-level discussion of why each test works and the type of failure that is targeted.>

<Specify any cutoffs used, and the meaning of these cutoffs.>

<Explain intermittent failures vs. permanent/persistent failures and how they are handled. Explain whether the source can deteriorate to a point where entropy claims can no longer be made.>

<Include a description of how errors are dealt with / signaled to the consuming application.>

## Conditioning

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 47, 48, 49, 91

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 21, 45, 46, 50, 51, 52, 53, 101, 108, 110, 111, 112, 113, 114

<Provide a detailed description of any conditioning. For vetted conditioning components, ADDITIONALLY include algorithm certificate numbers.>

<If keys are used, discuss how any value used to determine the key is not used as any other “input” to the conditioning component (and thus is not counted in that conditioning component’s ). Include details regarding key sizes used, keys used during algorithm testing (for vetted conditioning components), keys used in normal operation and when the keys are created (and that this creation occurs prior to any data being output from the entropy source).>

<Note: Algorithm validation testing was performed on vetted algorithm(s) prior to analysis.>

The conditioning chaining is shown in Figure 3. <Figure only necessary when there are two or more conditioning components and Figure 1 is not detailed enough.>

Figure 3. Conditioning Chain

# Noise Source Entropy Analysis

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B): 23, 36, 37

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B):33, 86

## Assumptions

The analysis is conducted under the following assumptions:

In General:

1. We perform this analysis under Kerckhoffs's principle, that is we assume that any attacker knows the entire design and has as much information regarding implementation as is useful.
2. Once data influences an output, we no longer assess this data as providing any entropy.
3. For the Noise Source:
4. The noise source state is protected from adversarial knowledge or influence to the greatest extent possible. <The methods for doing this are… >.
5. <Assumptions underlying the noise source analysis / assessment.>

## A Heuristic Entropy Estimate

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 9

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 35, 38, 95, 96, 97, 99, 100, 106, 107, 115, 116, 117, 122

<Here is where the stochastic model and/or technical argument is presented in adequate detail so that the analysis can be understood and the results could be replicated; we’ll call this here. The technical argument supporting the expected value must be based on the description of the source of unpredictability within the noise source and how the noise source outputs vary depending on this identified unpredictability. Statistical testing may be used to establish parameters referenced within this argument, but the value can’t be the result of a general statistical testing process that does not account for the design of the noise source. If the noise source produces a min entropy per output that is dependent on some internal state, must reflect an entropy bound that can be justified in the average case and/or on a per-symbol basis with high probability. Extended details that would distract from the narrative can be presented in Appendices.>

<Make sure to explain what assumptions are being relied upon. In particular, for software sources (and some hardware sources) this should include what assumptions are supported by the specific OEs allow this analysis to hold true. OE characteristics that influence the estimate should be explicitly listed in Table 2 (e.g., memory configuration, clock speed, processor model, the type of storage present, etc.)>

… by the above, we thus have characterized our heuristic min entropy estimate

<Optional per IG 7.18: Why it is believed that the entropy rate does not change significantly during normal operation?>

<Describe how the digitization process does not obscure the statistical properties of the raw noise source. (Recall that digitization includes combining outputs of noise source copies.)>

<If an IID claim is being made, add further information as necessary to show that independence and identical distribution are substantiated separately. Consider a possible deterioration of the source’s entropy generation pattern due to mechanical or environmental changes or to the timing variations in human behavior.>

## The Impact of Health Testing Requirements on

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 116, 117

In order to establish an appropriate value for , we must also examine the largest that would meet SP 800-90B Section 4.5 Requirements…

<If it is necessary to reduce the entropy claim in order to satisfy the Health Testing requirements, that can occur here. Explain exactly how any such bound was calculated. If this is not necessary, then the prior section can be the direct source of >

# Statistical Testing

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B): 84, 94

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 86, 122

<Statistical testing conducted using the NIST tool was produced using version / commit # (NIST recommends using an explicitly released and versioned tool). All relevant output of this tool can be found in Appendix A.>

<Note: For ESV submissions, this section is likely to be minimal, as the reviewers will look at the ESV results, not the testing described in this section. In this case, use this section to address requirements without providing the output from the NIST tool.>

## Raw Data Set Description

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 25, 33, 35, 58

In order to attempt to characterize the stability of the noise source and provide a bound for its min entropy production within its supported conditions…

<Describe any use of multiple instances of the part. Include information identifying the hardware used.>

<Describe any use of Process-Voltage-Temperature (PVT) or entropy-relevant parameter range testing.>

<Customer> provided r sample sets of raw data, with N million samples in each sample set.

Each of these sample sets are the sequential raw data output from the <Target> noise source. These r sample sets are expected to allow the testing to characterize the full range of operations within the expected environmental and process envelope.

Table 3. Specified Entropy Source Conditions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data Set Label | Parameter 1 | Parameter 2 | Parameter 3... | Raw Data Samples |
| ... | ... | ... | ... |  |

## Raw Data Testing, Formatting, and Extraction

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 1, 2, 29, 54, 55, 56, 59, 60, 89

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 10, 24, 98

This data was tested using m bit(s) per test symbol, in the order produced…

<Provide a description of the raw data. What is its data format?>

<Provide a description of how raw data is extracted from the device, and why this procedure is expected to produce a raw data sample that is expected to reflect the normal operation of the noise source (e.g., the sample rate is the same as when the entropy source is producing data for output). Recall that a sequential dataset of at least 1,000,000 sample values must be obtained directly from the noise source. Concatenation of several smaller sets of consecutive samples is allowed but must contain at least 1,000 samples.>

<Provide a description of why this procedure does not interfere with the noise source (e.g., is not expected to change the behavior of the noise source), and how the data was formatted for use by the 90B tool. If it is necessary to translate the data or map it down, describe this process here. If the original alphabet size was greater than 256 and it was reduced to meet SP 800-90B requirements, note this.>

<Document who performed the raw data extraction process, and describe the procedures required for this data extraction in Appendix F. This should also include any required vendor attestation documentation.>

## IID Testing

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 7, 10, 95, 96, 99, 100, 106, 107

<If an IID source is claimed, or the source’s design is IID, then it can be useful to present IID testing results here. If this section is omitted, please state that the source is non-IID directly.>

In order to meaningfully test these large data sets across the r identified conditions, we broke up each sample set of N million samples into N sample sets of 1 million samples each, and ran the IID tests for each of these 1 million sample sets.

In SP 800-90B, each IID test is designed to have a false reject rate of 1/1000. One can use the binomial distribution to establish how many failures for each data set would be expected for a p-value of 0.01. If we denote the CDF of the Binomial Distribution with parameters p=1/1000, n=N as (so, we are tracking failures of the test), we find the first integer k such that; this is the largest number of failures that are consistent with the p-value of 0.01. Through this, we find that N tests can be viewed as having passed so long as there were C or fewer failures in the N instances of that specific IID test.

The results are presented in Table 4.

Table 4. IID Test Results Across Provided Conditions

|  |  |  |
| --- | --- | --- |
| Data Set Label | Verdict | Observed Failures |
| ... | IID or Non-IID | None or list tests, e.g.,Excursion Test (Passed 98 / 100)Increases Directional Run Test (Passed 98 / 100)Chi-Square Goodness-of-Fit Test (Passed 82 / 100) |

The IID testing shows… <This should be interpreted as… An IID claim IS OR IS NOT being made here.>

## Statistical Assessment of Raw Data

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 8

[NIST SHALL] Requirement IDs that may partially be addressed in in any subsection below (see Appendix B): 10, 34, 35

### The -Stabilized Result

<This section presents an analysis approach which may be helpful, but is not required.>

For a fixed noise source with fixed entropy-relevant parameters, a min entropy estimator’s assessment conforms to some fixed distribution. It’s hard to comment on this distribution given only a single result, and sometimes this distribution is unhelpfully wide, which risks intermittent “downstream” validation failures. As such, we produce -stabilized assessments, as described in [Hill 2020].

In this procedure we characterize this assessment distribution on a per-estimator basis. We ultimately need to express our results using a single assessment per estimator, so we want to produce a summary statistic for this estimator assessment distribution. This summary statistic is intended to represent the underlying distribution more meaningfully than a single assessment would be expected to (as a single assessment is just a single value drawn from the assessment distribution). This summary statistic is taken as the overall estimator assessment across all of the performed rounds of each estimator. We then take the minimum overall summary statistic assessment across all the estimators as the overall -stabilized result.

The more rounds of assessments that are done, the more stable the result is, and the less entropy is lost to statistical artifacts. Of course, doing more assessments requires more data, so there are practical tradeoffs.

The summary statistic is taken to be the median for all the estimators other than the (binary) Markov estimator. The median is chosen because it is central; that is, it is a value that has the smallest expected L1 distance from a value selected from this assessment distribution. Estimates for the median are fairly stable, and don’t require a substantial number of samples to estimate accurately.

Unfortunately, a median of Markov estimator results isn’t directly comparable to the medians of all the other estimators’ results (for which two-sided 99% confidence intervals are used). As such, we instead estimate the 0.5th percentile for the Markov estimator, which makes the summary statistic for the Markov estimator directly comparable to all of the other estimators’ summary statistics.

In order to characterize this distribution, we subdivide the large raw data set into subsets of 1 million samples each. Each of these subsets is then separately analyzed using the SP 800-90B non-IID[[1]](#footnote-2) track, producing assessment results per estimator.

In all cases, we establish 99% bootstrap confidence intervals for the sought percentile. The bootstrap procedure that we use is described in Efron and Hastie [EH 2016, Chapters 10-11]. We generate a BCa Bootstrap Confidence Interval when this value is defined. If this value is not defined, then we fall back to a BC Bootstrap Confidence Interval (if the acceleration is undefined but the bias is defined) or a Percentile Bootstrap Confidence Interval (if the bias is undefined). In all cases, we perform 15,000 rounds of bootstrap sampling.

### The Large Block Assessment

For each raw data set, we also perform a single *Large Block Assessment* (LBA), where the full data set is assessed as a single data set using the NIST SP 800-90B tool.

### The Overall Statistical Assessment

These assessments can be combined in a way that is compliant with SP 800-90B.

Calculate the 𝑟-stabilized assessment using disjoint subsets of the raw data set.

Perform a single Large Block Assessment on the full raw data set.

The final assessment is the minimum of the 𝑟-stabilized assessment and the Large Block Assessment.

This is mappable to the SP 800-90B process. First note that the Large Block Assessment is exactly the SP 800-90B statistical assessment process but with a very large data set (which is allowed in SP 800-90B). If the -stabilized assessment is lower than the Large Block Assessment, this can be thought of as reducing the vendor’s value.

### Statistical Assessment Results

The statistical testing results are summarized in the following table. The bolded assessment is the minimum for any of the assessed conditions.

Table 5. Statistical Assessment Results[[2]](#footnote-3)

|  |  |
| --- | --- |
| Data Set Label | Assessed Min Entropy |
| … | <result> |

We thus adopt an initial min entropy assessment of **.**

Similarly, the resulting **.**

## Restart Testing

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 5, 6, 11, 12, 13, 14, 32, 92

<Customer/Lab> extracted restart data as described in SP 800-90B Sections 3.1.1 and 3.1.4. The entropy source was restarted 1000 times. For each restart, 1000 consecutive samples were collected directly from the noise source immediately when it was ready and able under real-world conditions.

<Describe what “restart” means for this source under normal, real-world operating conditions and the process which was applied during restart testing.>

This was drawn from an instance of the entropy source in its nominal condition (parameter 1, parameter 2, parameter 3, …).

Table 6. Restart Test Results

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Initial Entropy () |  |  | Restart Sanity Test Results |  |  |  |
| … | … | … | Pass/Fail | … | … | … |

<Summarize what H is as a result.>

This testing <passed/failed>, and the column and row assessments both <…> (see Table 6), so as directed in SP 800-90B Section 3.1.4.2, we have .

See Appendix A for the output of the NIST tool.

# Health Testing and Error Modes

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 63, 64, 71, 72, 73

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 86, 90

## Assumptions

1. For the Health Tests:
2. <Any assumptions underlying the health testing analysis / assessment.>

## Health Tests

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 61, 62

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B):70, 78, 79 (any subsection dealing with the APT), 120

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 67, 75, 76, 118, 119, 121

SP 800-90B requires three types of health tests:

Start-up health tests:

<health tests>

Continuous health tests:

<health tests>

On-demand health tests

<health tests>

<How are samples drawn during start-up tests not available for normal operations until the tests are complete?>

<How many consecutive samples are used within start-up tests prior to allowing output from the noise source )?>

<How are samples collected during on-demand tests not available for normal operations until the tests are complete? Does this include at least the same testing done by the start-up tests?>

### Health Test 1

<If multiple copies of the same noise source are used, describe the relationship between the data that is being tested and the output of each noise source copy, and describe how combining these copies within the digitization process does not conceal noise source failures from the health tests. >

<Describe false positive rate, how this was established, and the assumptions underlying this rate. Provide the calculations that tie the selected cutoff to the selected false positive rate.>

<If APT, describe window size W. Cutoff .>

### Health Test 2…

…

## Anticipated Failure Modes

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B): 77

[NIST SHALL] Requirement IDs that may partially be addressed in any subsection below (see Appendix B): 97, 118, 119

Various component failure and inappropriate parameter selections can yield a variety of failure modes…

### Failure Mode 1

<What is the failure mode? When in this failure mode, what is the false accept probabilities for the relevant health tests? Generally explain how each failure mode is detected using the included health tests.>

### Failure Mode 2…

…

## Requirements for Developer-Defined Alternatives to the Continuous Health Tests

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B): 65, 123, 124

<If the entropy source does not include the Approved health tests, then additional arguments are required.>

### SP 800-90B Section 4.5 Criterion (a)

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 80

SP 800-90B Section 4.5 Requirement (a) is analogous to the Repetition Count Test. To satisfy this requirement, we need to show that if a single value appears more than consecutive times, then the health test indicates a failure with probability 99% or more.

<Include argument here, if applicable. Make sure to address the health tests’ power / false accept rate while in the described failure mode.>

<If simulation is used as proof, specify how the data used within this simulation was created. At least 1 million rounds of simulation are needed for each simulated health test, and there must be sufficient simulation rounds so that at least five health test failures are observed for each health test.>

### SP 800-90B Section 4.5 Criterion (b)

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 81

SP 800-90B Section 4.5 Requirement (b) is analogous to the Adaptive Proportion Test. To satisfy this requirement, we need to show that if the entropy output of the source is reduced by a factor of 2, then after 50,000 samples of this reduced-entropy data, the health test detects a failure with probability 50% or more.

<Include argument here, if applicable. Make sure to address the health tests’ power / false accept rate while in the described failure mode.>

<If simulation is used as proof, specify how the data used within this simulation was created. At least 1 million rounds of simulation are needed for each simulated health test, and there must be sufficient simulation rounds so that at least five health test failures are observed for each health test.>

# Conditioning Analysis

[NIST SHALL] Requirement IDs that may be addressed in any subsection below (see Appendix B): 86, 102, 103, 105, 106, 109.

<Include details regarding vetted conditioning, non-vetted conditioning, chaining, chaining order, algorithms/key sizes, overall input/output sizes, and supplemental data (for vetted conditioning components).>

## Assumptions

1. For the Conditioning Function:
2. <Any assumptions underlying the conditioning analysis / assessment.>

## Design-Based Conditioning Analysis for Non-Vetted Conditioning

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 45, 51, 52, 53, 104, 106, 107, 113, 114

<Any non-vetted conditioning is analyzed here, resulting in a design-based bound for the conditioning, . Use subsections if there are multiple non-vetted components.>

### Non-Vetted Component 1

<Give mathematical evidence to show that the component does not significantly reduce the entropy rate. Provide justification about why the component does not act poorly when the noise source data is not independent.>

<If the bijective property is being claimed, demonstrate that the mapping performed by the conditioning function is bijective. Specify a detailed procedure for reversing any conditioning function that is claimed to be bijective.>

<Explain how there is no truncation.>

<For a component with state and where the primary noise source is not independent, justify why the reduction of the component’s output entropy due to the cancellation of mutual information present in both the data input to the conditioning component and the retained state does not result in the output entropy of the component being below its assessed value ().>

### Non-Vetted Component 2…

…

## SP 800-90B Conditioning Chain Analysis

[NIST SHALL] Requirement IDs to be addressed in any subsection below (see Appendix B): 3, 4, 15, 16, 17, 18, 19, 57, 102, 103, 105

[NIST SHALL] Requirement IDs that may partially be addressed in in any subsection below (see Appendix B): 20, 21, 41, 43, 45, 46, 50, 51, 101, 104, 108, 109, 110, 111, 112, 113, 114

<If there is just one conditioning component, this section could be titled “Conditioning Analysis”.>

<If additional noise sources are available, discuss how accounts only for data from the primary noise source.>

Table 7. Conditioning Chain

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Conditioning Component | Vetted? (Algorithm Certificate #) | Input Data Source | Supplemental Data Source | Bijective? | Retains State? |
| Component 1 (Ex: Vetted) | Y (Cert #) | … | … | Y/N | Y/N |
| Component 2 (Ex: Non-vetted) | N | … | … | Y/N | Y/N |
| Component 3… | Y (Cert #) / N | … | … | Y/N | Y/N |

### Conditioning Component 1 (Example: Vetted)

The vetted conditioning function <HMAC, CMAC, CBC-MAC (as per SP 800-90B Appendix F), Hash Function, Hash\_df, or Block\_Cipher\_df> from SP 800-90B Section 3.1.5.1.1 is used.

The relevant parameters for the specified mode of use of this conditioning function yield the conditioning constants described in Table 8. Given these values, we can directly estimate an assessed output entropy as per SP 800-90B Sections 3.1.5.1.2 and 3.1.5.2.

Table 8. SP 800-90B Conditioning Summary for Component 1

|  |  |
| --- | --- |
| Output Bit | Credited Bits |
| Symbols Input (w) |  |
| Symbol Width () |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

<The Output\_Entropy function is described in SP 800-90B Section 3.1.5.1.2. If this calculation is performed using something other than the NIST ea\_conditioning tool, provide a complete description of how the calculation was performed.>

<If supplemental data is used, discuss how the presence of supplemental data is not credited toward or .>

### Conditioning Component 2... (Example: Non-vetted)

<Customer> provided one sample set of sequential conditioned data <of at least 1,000,000 outputs> drawn from conditioning component 2 within an instance of the entropy source during normal operating conditions. This sample was assessed as a bitstring (as directed in SP 800-90B Section 3.1.5.2). See Appendix A for the output of the test tool associated with this testing.

Table 9. Conditioned Test Results for Component 2 (if non-vetted)

|  |  |  |  |
| --- | --- | --- | --- |
| Sample Size (bytes) | Sample Size(bits) |  |  |
| … | … |  |  |

The relevant parameters for the specified mode of use of this conditioning function yield the conditioning constants described in Table 10. Given these values, we can directly estimate an assessed output entropy as per SP 800-90B Sections 3.1.5.1.2 and 3.1.5.2.

Table 10. SP 800-90B Conditioning Summary for Component 2

|  |  |
| --- | --- |
| Output Bit | Credited Bits |
| Symbols Input (w) |  |
| Symbol Width () |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | (If non-vetted) |
|  | (If non-vetted) |
|  |  |

<Describe how is established by design analysis and application of SP 800-90B Appendix E.>

<Discuss how truncation is not performed during the conditioning phase.>

Table 11. Non-Vetted Conditioning Component Entropy Summary

|  |  |
| --- | --- |
| (per block) | Conditioning Component (per block) |
|  |  |

<The minimum of these two claims can be claimed as the basis for in the next stage / output from the conditioning chain.>

### Conditioning Component 3…

### Conditioning Chain Results Summary

We thus claim an output of at least bits of min entropy per byte output from the entropy source.

# Conclusion

[NIST SHALL] Requirement IDs to be addressed in this section (see Appendix B): 93

[NIST SHALL] Requirement IDs that may partially be addressed in this section (see Appendix B): 20

We claim a min entropy output of at least bits of min entropy per <block size>.

<These blocks are the output of a <vetted/non-vetted> conditioning function, and <can/cannot> be subdivided further (as per the requirements of SP 800-90B).>

If this entropy source is used to seed a compliant DRBG, then the seeding requirements summarized in Table 12 must be met.

Table 12. Seeding Requirements for Security Strengths

|  |  |  |
| --- | --- | --- |
| DRBG Security Strength (bits) | Blocks Required(Nonce Provided) | Blocks Required(Random Nonce) |
| 112 | … | … |
| 128 | … | … |
| 192 | … | … |
| 256 | … | … |

# References

<Add references relevant to the design and assessment approach.>

<Include links to any relevant open-source components>

[EH 2016] Bradley Efron, Trevor Hastie. *Computer Age Statistical Inference*. 2016.

[Hill 2020] Joshua E. Hill. *SP 800-90B Refinements: Validation Process, Estimator Confidence Intervals, and Assessment Stability*. ICMC 2020.

[IG] *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program*. February 14, 2022.

[NIST SHALL] NIST CMVP. *90B-Shall-Statements*. <https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/esv/90B%20Shall%20Statements.xlsx>.

[SP 800-90B] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish and Mike Boyle. *Recommendation for the Entropy Sources Used for Random Bit Generation*. January 2018.

1. NIST Tool Output

<This appendix is not necessary when submitting using the ESV program.>

All testing associated with outputs included here was conducted using the version of the NIST tool referenced in Section 4.

## Smallest Raw Data Large Block Assessment

<NIST TOOL OUTPUT>

## Conditioned Data Assessment

<NIST TOOL OUTPUT>

## SP 800-90B Conditioning Calculation

<NIST TOOL OUTPUT>

## Restart Testing

<NIST TOOL OUTPUT>

1. SP 800-90B and FIPS 140 Requirement Mapping

## SP 800-90B “Shall” Requirements

The table below includes the “shall” requirements from SP 800-90B Sections 3 and 4, as identified in NIST’s “Shall Statements” list [NIST SHALL]. Other section labels used in the “Addressed in Section” column are references to sections of this report, unless otherwise indicated. Purple text in the “Addressed in Section” column indicates verification tasks that are outside the scope of this report.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID # | SP 800-90B Section and Location | Statement | Requirement Status | Addressed in Section |
| 1 | §3.1.1Item (1) | A sequential dataset of at least 1,000,000 sample values obtained directly from the noise source (i.e., raw data) **shall** be collected for validation | Required | §4.2 |
| 2 | §3.1.1Item (1) | If the generation of 1,000,000 consecutive samples is not possible, the concatenation of several smaller sets of consecutive samples (generated using the same noise source) is allowed. Smaller sets **shall** contain at least 1,000 samples. The concatenated dataset **shall** contain at least 1,000,000 samples. | Required | §4.2 |
| 3 | §3.1.1Item (2) | If the entropy source includes a conditioning component that is not listed in Section 3.1.5.1.1, a conditioned sequential dataset of at least 1,000,000 consecutive conditioning component outputs **shall** be collected for validation. | Required | §6.3 and its subsections |
| 4 | §3.1.1Item (2) | The output of the conditioning component **shall** be concatenated in the order in which it was generated and treated as a binary string for testing purposes. | Required | §6.3 and its subsections |
| 5 | §3.1.1Item (3) | For the restart tests (see Section 3.1.4), the entropy source must be restarted 1,000 times; for each restart, 1,000 consecutive samples **shall** be collected directly from the noise source. | Required | §4.5 |
| 6 | §3.1.1Item (3) | The restart data **shall** be extracted whenever the noise source is ready and able to provide data that can be used for producing entropy source output. | Required | §4.5 |
| 7 | §3.1.2Item (1) | The submitter makes an IID claim on the noise source, based on the submitter’s analysis of the design. The submitter **shall** provide rationale for the IID claim. | Only required for sources making an IID claim | §1, §2.1, §4.3 |
| 8 | §3.1.2Final paragraph | If any of these conditions (IID claim rationale, IID assumption verified by statistical tests in Section 5 on raw data, restart data, and any non-vetted conditioning component data) are not met, the estimation process **shall** follow the non-IID track. | Required | §4.4 |
| 9 | §3.1.3Paragraph 1 | The submitter **shall** provide an entropy estimate for the noise source outputs, which is based on the submitter’s analysis of the noise source | Required | §3.2 |
| 10 | §3.1.3Paragraph 2 | If the alphabet size is greater than 256, it **shall** be reduced to at most 256 symbols (see Section 6.4). | Required | §4.2, §4.3, §4.4 |
| 11 | §3.1.4Paragraph 2 | The submitter **shall** define the restart process suitable for the submission. | Required | §4.5 |
| 12 | §3.1.4Paragraph 2 | This process **shall** simulate the restart process expected in real-world use (e.g., the outputs are not generated until after the start-up tests are complete; see Section 4.2). | Required | §4.5 |
| 13 | §3.1.4.1Paragraph 1 | To construct restart data, the entropy source **shall** be restarted r = 1,000 times; for each restart, c = 1,000 consecutive samples **shall** be collected directly from the noise source. | Required | §4.5 |
| 14 | §3.1.4.1Paragraph 1 | The collection of the data **shall** be done as soon as the entropy source is ready to produce outputs for real-world use (e.g., after start-up tests). | Required | §4.5 |
| 15 | §3.1.5Paragraph 1 | The size of the input and the output of the conditioning component in bits, denoted as n\_in and n\_out, respectively, **shall** be fixed and **shall** be specified by the submitter. | Required | §6.3 and its subsections |
| 16 | §3.1.5Paragraph 1 | The size of the conditioning component input **shall** be a multiple of the size of the noise source output. | Required[[3]](#footnote-4) | §6.3 and its subsections |
| 17 | §3.1.5.1.2Paragraph 2 | When additional noise sources are available, the length of the input (n\_in) **shall** only include the inputs from the primary noise source. | Required | §6.3 and its subsections |
| 18 | §3.1.5.2Paragraph 1 | For non-vetted conditioning components, the entropy in the output depends on the entropy and size of the input (h\_in and n\_in), the size of the output (n\_out), and the size of the narrowest internal width (nw) and the entropy of the conditioned sequential dataset (as described in item 2 of Section 3.1.1), which **shall** be computed using the methods described in either Section 6.1 (for IID data) or Section 6.2 (for non-IID data). | Required | §6.3 and its subsections |
| 19 | §3.1.5.2Paragraph 2 | The output of the conditioning component (n\_out) **shall** be treated as a binary string, for purposes of the entropy estimation. | Required | §6.3 and its subsections |
| 20 | §3.1.5.2, Final Paragraph | Note that truncating subsequent to the use of a non-vetted conditioning component **shall** not be performed before providing output from the entropy source. | Required | §6.3 and its subsections, §7 |
| 21 | §3.1.6, Sole Requirement | This Recommendation allows one to concatenate the outputs of the additional noise sources to the primary noise source to generate input to the conditioning component. In such cases, vetted conditioning components **shall** be used. No entropy is credited from the outputs of the additional noise sources. | Required | §2.3, §6.3 and its subsections |
| 22 | §3.2.1Requirement 1 | The entire design of the entropy source **shall** be documented, including the interaction of the components specified in Section 2.2. | Required | §2 and its subsections |
| 23 | §3.2.1Requirement 1 | The documentation **shall** justify why the entropy source can be relied upon to produce bits with entropy. | Required | §3 and its subsections  |
| 24 | §3.2.1Requirement 2 | Documentation **shall** describe the operation of the entropy source, including how the entropy source works, and how to obtain data from within the entropy source for validation testing. | Required | §2 and its subsections, §4.2 |
| 25 | §3.2.1Requirement 3 | Documentation **shall** describe the range of operating conditions (e.g., temperature range, voltages, system activity, etc.) under which the entropy source is claimed to operate correctly. | Required | §1.1, §4.1 |
| 26 | §3.2.1Requirement 4 | The entropy source **shall** have a well-defined (conceptual) security boundary. | Required | §1 |
| 27 | §3.2.1Requirement 4 | This security boundary **shall** be documented; the documentation **shall** include a description of the content of the security boundary. | Required | §1 |
| 28 | §3.2.1Requirement 5 | When a conditioning component is included in the entropy source, the output from the entropy source is the output of the conditioning component, and an additional interface is required to access the noise-source output. In this case, the noise-source output **shall** be accessible via the interface during validation testing, but the interface may be disabled otherwise. | Required | §2.1 |
| 29 | §3.2.1Requirement 5 | The designer **shall** fully document the method used to get access to the raw noise source samples. | Required | §4.2 |
| 30 | §3.2.1Requirement 5 | If the noise-source interface is not disabled during normal operation, any noise-source output using this interface **shall** not be provided to the conditioning component for processing and eventual output as normal entropy-source output. | Required | §2.1 |
| 31 | §3.2.1Requirement 6 | The entropy source may restrict access to raw noise source samples to special circumstances that are not available to users in the field, and the documentation **shall** explain why this restriction is not expected to substantially alter the behavior of the entropy source as tested during validation. | See Requirements 56 and 60. | §2.1 |
| 32 | §3.2.1Requirement 7 | Documentation **shall** contain a description of the restarting process applied during the restart tests. | Required | §4.5 |
| 33 | §3.2.2Requirement 1 | The operation of the noise source **shall** be documented; This documentation **shall** include a description of how the noise source works, where the unpredictability comes from, and rationale for why the noise source provides acceptable entropy output, and should reference relevant, existing research and literature. | Required | §2.1, §3 and its subsections, §4.1 |
| 34 | §3.2.2Requirement 2 | The behavior of the noise source **shall** be stationary (i.e., the probability distributions of the noise source outputs do not change when shifted in time). | Optional (Per IG 7.18 Additional Comment #2.) | §1.1, §2.1, §4.4 |
| 35 | §3.2.2Requirement 2 | Documentation **shall** include why it is believed that the entropy rate does not change significantly during normal operation. | Optional(Per IG 7.18 Additional Comment #2.) | §3.2, §4.1, §4.4 and its subsections |
| 36 | §3.2.2Requirement 3 | Documentation **shall** provide an explicit statement of the expected entropy provided by the noise source outputs and provide a technical argument for why the noise source can support that entropy rate. | Required only for the primary noise source. | §3 and its subsections |
| 37 | §3.2.2Requirement 4 | The noise source state **shall** be protected from adversarial knowledge or influence to the greatest extent possible. The methods used for this **shall** be documented, including a description of the (conceptual) security boundary’s role in protecting the noise source from adversarial observation or influence. | Required | §3 and its subsections |
| 38 | §3.2.2Requirement 5 | Although the noise source is not required to produce unbiased and independent outputs, it **shall** exhibit random behavior; i.e., the output shall not be definable by any known algorithmic rule. | See Requirements 33 and 36. | §2.1, §3.2 |
| 39 | §3.2.2Requirement 5 | Documentation **shall** indicate whether the noise source produces IID data or non-IID data. This claim will be used in determining the test path followed during validation. | See Requirements 7 and 8. | §2.1 |
| 40 | §3.2.2Requirement 5 | If the submitter makes an IID claim, documentation **shall** include rationale for the claim. | See Requirements 7 and 8. | §2.1 |
| 41 | §3.2.2Requirement 6 | The noise source **shall** generate fixed-length bitstrings. | Required | §2.1, §6.3 and its subsections |
| 42 | §3.2.2Requirement 6 | A description of the output space of the noise source **shall** be provided. | Required | §2.1 |
| 43 | §3.2.2Requirement 6 | Documentation **shall** specify the fixed symbol size (in bits) and the list (or range) of all possible outputs from each noise source. | Required | §2.1, §6.3 and its subsections |
| 44 | §3.2.2Requirement 7 | If additional noise source outputs to increase security are used, a document that describes the additional noise sources **shall** be included. | Required | §2.1 |
| 45 | §3.2.3Requirement 1 | The submitter **shall** document which conditioning component is used and the details about its implementation (e.g., the hash function and/or key size used). | Required | §2.3, §6.2, §6.3 and its subsections |
| 46 | §3.2.3Requirement 1 | Documentation **shall** include the input and the output sizes (n\_in and n\_out). | Required | §2.3, §6.3 and its subsections |
| 47 | §3.2.3Requirement 2 | If the entropy source uses a vetted conditioning component as listed in Section 3.1.5.1.1, the implementation of the component **shall** be tested to obtain assurance of correctness before subsequent testing of the entropy source. | Required | §2.3 |
| 48 | §3.2.3Requirement 2 | The submitter **shall** specify any keys used to test the correctness of the conditioning component implementation during validation testing.  | Required if the implementation requires a specific key. Otherwise, this is not applicable. | §2.3 |
| 49 | §3.2.3Requirement 3 | The key **shall** be determined before any outputs are generated from the conditioning component. | Required if the implementation requires a key to be generated from the noise source. Otherwise, this is not applicable. | §2.3 |
| 50 | §3.2.3Requirement 4 | Any value which is used to determine the key **shall** **not** be used as any other input to the conditioning component. The input entropy to the conditioning component (h\_in) **shall** **not** include any entropy provided to the key of a keyed function.  | Required if the implementation requires a key to be generated from the noise source. Otherwise, this is not applicable. | §2.3, §6.3 and its subsections |
| 51 | §3.2.3Requirement 5 | For entropy sources containing a conditioning component that is not listed in Section 3.1.5.1.1, a description of the conditioning component **shall** be provided. Documentation **shall** state the narrowest internal width (nw) and the size of the output blocks from the conditioning component. | Required only for non-vetted conditioning components. | §2.3, §6.2, §6.3 and its subsections |
| 52 | §3.2.3Requirement 5 | The submitter **shall** provide mathematical evidence that the component is suitable to be used to condition the noise source output, and does not significantly reduce the entropy rate of the entropy source output. | Optional(This statement only applies to non-vetted conditioning components. See Requirement 51.) | §2.3, §6.2 |
| 53 | §3.2.3Requirement 5 | The submitter **shall** also provide a justification about why the conditioning component does not act poorly when the noise source data is not independent. | Optional(This statement only applies to non-vetted conditioning components. See Requirement 51.) | §2.3, §6.2 |
| 54 | §3.2.4Requirement 1 | The data collection for entropy estimation **shall** be performed in one of the three ways described below: By the submitter with a witness from the testing lab, or; By the testing lab itself; or Prepared by the submitter in advance of testing, along with the following documentation: a specification of the data generation process, and a signed document that attests that the specification was followed. | Required  | §4.2, Appendix F |
| 55 | §3.2.4Requirement 2 | Data collected from the noise source for validation testing **shall** be raw output values | Required  | §4.2 |
| 56 | §3.2.4Requirement 3 | The data collection process **shall not** require a detailed knowledge of the noise source or intrusive actions that may alter the behavior of the noise source (e.g., drilling into the device). | Optional(As long as the process is reproducible. Must provide justification on how this does not alter the behavior of the noise source.) | §4.2 |
| 57 | §3.2.4Requirement 4 | Data **shall** be collected from the noise source and any conditioning component that is not listed in Section 3.1.5.1.1 (if used) under normal operating conditions. | Required | §6.3 and its subsections |
| 58 | §3.2.4Requirement 5 | Data **shall** be collected from the entropy source under validation. Any relevant version of the hardware or software updates shall be associated with the data. | Required | §1.1, §4.1 |
| 59 | §3.2.4Requirement 6 | Documentation of the data collection method **shall** be provided so that a lab or submitter can perform (or replicate) the collection process at a later time, if necessary. | Required | §4.2, Appendix F |
| 60 | §3.2.4Requirement 7 | Documentation explaining why the data collection method does not interfere with the noise source **shall** be provided. | Required | §4.2 |
| 61 | §4.2Paragraph 2 | The samples drawn from the noise source during the startup tests **shall not** be available for normal operations until the tests are completed; | Required | §2.2, §5.2 |
| 62 | §4.2Paragraph 5 | Samples collected from the noise source during on-demand health tests **shall not** be available for use until the tests are completed | Required | §2.2, §5.2 |
| 63 | §4.3Paragraph 1 | Health tests on the noise source are a required component of an entropy source. The health tests **shall** include both continuous and start-up tests. | Required | §2.2, §5 |
| 64 | §4.3Requirement 1 | The continuous tests **shall** include either: a. The approved continuous health tests, described in Section 4.4, or b. Some developer-defined tests that meet the requirements for a substitution of those approved tests, as described in Section 4.5. | Required | §2.2, §5 |
| 65 | §4.3Requirement 1 | If developer-defined health tests are used in place of any of the approved health tests, the tester **shall** verify that the implemented tests detect the failure conditions detected by the approved continuous health tests, as described in Section 4.4. | Required | §5.4 and its subsections |
| 66 | §4.3Requirement 2 | When the health tests fail, the entropy source **shall** notify the consuming application (e.g., the RBG) of the error condition. | Required only if the consuming application requires more entropy than is available in a buffer (e.g. RBG is reseeding and has exceeded the amount of entropy previously outputted from the entropy source). | §2.2 |
| 67 | §4.3Requirement 2 | The developer is allowed to define different cutoff values to detect intermittent and persistent failures. If so, these values (with corresponding false alarm probabilities) **shall** be specified in the submission documentation. | Required | §2.2, §5.2 and its subsections |
| 68 | §4.3Requirement 2 | If the entropy source detects intermittent failures and allows the noise source to return to normal functioning, the designer **shall** provide evidence that: a) The intermittent failures handled in this way are indeed extremely likely to be intermittent failures; and b) the tests will detect a permanent failure when one occurs, and will ultimately signal an error condition to the consuming application and cease operation. | Required | §2.2 |
| 69 | §4.3Requirement 2 | In the case where a persistent failure is detected, the entropy source **shall not** produce any outputs. | Required | §2.2 |
| 70 | §4.3Requirement 3 | The submitter **shall** specify and document a false positive probability suitable for their application. | Required; specify value within the range of 2^-40 to 2^-20, or justify value outside of range. | §5.2 and its subsections |
| 71 | §4.3Requirement 4 | The entropy source's startup tests **shall** run the continuous health tests over at least 1024 consecutive samples. | Required | §2.2, §5 |
| 72 | §4.3Requirement 5 | The entropy source **shall** support on-demand testing. The on-demand tests shall include at least the same testing done by the start-up tests. | Required | §2.2, §5 |
| 73 | §4.3Requirement 5 | The documentation **shall** specify the approach used for on-demand testing. | Required | §2.2, §5 |
| 74 | §4.3Requirement 6 | Health tests **shall** be performed on the noise source samples before any conditioning is done. | Required | §2.2 |
| 75 | §4.3Requirement 7 | The submitter **shall** provide documentation that specifies all entropy source health tests and their rationale. | Required | §2.2, §5.2 and its subsections |
| 76 | §4.3Requirement 7 | The documentation **shall** include a description of the health tests, source code, the rate and conditions under which each health test is performed (e.g., at power-up, continuously, or on-demand), and include rationale indicating why each test is believed to be appropriate for detecting one or more failures in the noise source. | Required | §2.2, §5.2 and its subsections |
| 77 | §4.3Requirement 8 | The submitter **shall** provide documentation of any known or suspected noise source failure modes (e.g., the noise source starts producing periodic outputs like 101…01), and **shall** include developer-defined continuous tests to detect those failures. | Optional | §5.3 and its subsections |
| 78 | §4.4Paragraph 3 | The developer of the entropy source **shall** determine a reasonable probability of type I error (and corresponding cutoff values), based the details of the entropy source and its consuming application. | Required | §5.2 and its subsections |
| 79 | §4.4.2Paragraph 2 | The window size W is selected based on the alphabet size, and **shall** be assigned to 1024 if the noise source is binary (that is, the noise source produces only two distinct values) and 512 if the noise source is not binary (that is, the noise source produces more than two distinct values). | Optional(The window size must be specified, but other values than 1024 for binary samples and 512 for non-binary samples may be allowed with justification.) | §5.2 and its subsections dealing with the APT test |
| 80 | §4.5Criteria (a) | If a single value appears more than ceil(100/H) consecutive times in a row in the sequence of noise source samples, the test **shall** detect this with a probability of at least 99%. | Required | §5.4.1 |
| 81 | §4.5Criteria (b) | If the noise source's behavior changes so that the probability of observing a specific sample value increases to at least P\* = 2^(−H/2), then the test **shall** detect this change with a probability of at least 50% when examining 50,000 consecutive samples from this degraded source. | Required | §5.4.2 |

## FIPS 140 IG Requirement Mapping

This entropy assessment document justifies compliance to the FIPS 140-2 IGs 7.18/7.19 because this is how these requirements are referred to within NIST’s “Shall Statements” identification [NIST SHALL]. These same requirements are present within FIPS 140-3 IGs D.J and D.K. This report can be used to support both FIPS 140-2 and FIPS 140-3 validations.

Purple text in the “Addressed in Section” column indicates verification tasks that are outside the scope of this report.

### IG 7.18

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID # | IG 7.18 Location | Statement | Requirement Status | Addressed in Section |
| 82 | Resolution Paragraph 1 | If the test report for a cryptographic module is submitted for validation after November 7, 2020 (that is, more than eighteen months after the original publication date of this Implementation Guidance) and if this module falls under one of the scenarios of IG 7.14 that require entropy estimation, then the module **shall** be tested for its compliance with SP 800-90B and IG 7.19. |  | Validation Process. |
| 83 | Resolution Paragraph 1 | The requirements represented by the “**shall**” statements in SP 800-90B apply and must be tested by the lab, with the possible exceptions as stated below in this Implementation Guidance and in IG 7.19. These requirements include running statistical tests on the raw entropy data, as explained in SP 800-90B. |  | Validation Process. |
| 84 | Resolution Paragraph 1 | Statistical testing **shall** be performed using a software tool available at https://github.com/usnistgov/SP800-90B\_EntropyAssessment. |  | Validation Process. The version of the NIST 90B tool used is documented in §4. Statistical testing is described in §4 and its subsections. |
| 85 | Resolution Paragraph 2 | When claiming compliance with SP 800-90B to meet the requirements of AS.07.13 and AS.07.16, the testing laboratory **shall** provide a PDF addendum to the submitted test report. |  | Validation Process. |
| 86 | Resolution Paragraph 2 | This addendum **shall** include a detailed logical diagram showing all components of an entropy source and the numerical results of various tests required by SP 800-90B. |  | §1, §2, §3, §4, §5, §6, and their subsections |
| 87 | Resolution Paragraph 2 | The addendum **shall** contain both a rationale for why the final entropy assessment is consistent with both the SP 800-90B statistical tests and the required heuristic analysis of the entropy source, and a description of how the entropy source satisfies all of the SP 800-90B '**shall**' statements. |  | Validation Process. |
| 88 | Resolution Paragraph 2 | When a cryptographic module is validated for its compliance with SP 800-90B, the module’s validation certificate **shall** include one of the following entries on the approved algorithm line: ENT(P) or ENT(NP) where P stands for physical and NP for non-physical. |  | Validation Process. |
| 89 | Additional Comment 1 | In compliance with SP 800-90B, vendors **shall** provide access to the raw outputs of the entropy source. | Required | §4.2 |
| 90 | Additional Comment 2 | If the source may deteriorate to the point when the generation of the sufficient amount of entropy (sufficient to support the claims about the strengths of the generated cryptographic keys) can no longer be guaranteed, the module’s Security Policy **shall** explain what action is to be taken. | Required | §2.2, §5 and its subsectionsThe module’s Security Policy states the action to be taken. |
| 91 | Additional Comment 3 | The approved algorithms used in the vetted conditioning components **shall** be tested by the CAVP (if testing is available for them). This is a reiteration of a requirement from Section 3.1.5.1.2 of SP 800-90B. | Required | §2.3 |
| 92 | Additional Comment 4 | A restart test requirement from Section 3.1.4.3 of SP 800-90B needs to be addressed. A failure of a restart test does not automatically disqualify the module from being validated. Should this failure occur, the lab **shall** analyze the reason for a failure of the test and explain how the entropy requirement can be met in light of this failure. | Not required(Clause was put into IG 7.18 because there was a bug in the Entropy Assessment Tool. This has since been fixed, so this clause is no longer relevant.) | §4.5  |
| 93 | Additional Comment 6 | When entropy source testing to SP 800-90B is applicable, the module’s Security Policy **shall** document the overall amount of generated entropy and the estimated amount of entropy per the source’s output bit. |  | §7The module’s Security Policy states the amount of data output from the entropy source and its assessed entropy when used to instantiate or reseed approved DRBGs.  |
| 94 | Additional Comment 7 | The SP 800-90B testing tool’s version number will be made available to users of the tool. This version number **shall** be included in the lab’s Entropy Test Report. |  | The version of the NIST 90B tool used is documented in §4. Statistical testing is described in §4 and its subsections. |
| 95 | Additional Comment 9 | A claim of independence and that of an identical distribution **shall** be substantiated separately. | Required only for IID claims. | §2.1, §3.2, §4.3 |
| 96 | Additional Comment 9 | A claim of an identical distribution of the samples **shall** consider a possible deterioration of the source’s entropy generation pattern due to the mechanical or the environmental changes or to the timing variations in human behavior. | Required only for IID claims. | §2.1, §3.2, §4.3 |

### IG 7.19

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID # | IG 7.19 Location | Statement | Requirement Status | Addressed in Section |
| 97 | Resolution 1 | For Section 2.2.1, the vendor **shall** justify why all processing occurring within the digitization process does not conceal noise source failures from the health tests or obscure the statistical properties of the underlying raw noise output from this digitization process. | Required | §2.1, §3.2, §5.3 and its subsections |
| 98 | Resolution 1 | The tester **shall** provide a detailed description of all digitization processes used within the noise source and describe the format of the raw data that was tested. (See SP 800-90B Section 3.2.2 Requirement #3, and Section 4.3 Requirements #1, #6, #7, #8, and #9). | Required | §2.1, §4.2 |
| 99 | Resolution 2 | The testing laboratory **shall** evaluate the technical accuracy and completeness of any IID rationale made by the vendor | Required | Validation Process. §2.1, §3.2, §4.3 |
| 100 | Resolution 2 | If it is not possible for the vendor to produce such a rigorous proof and/or it is not possible for the laboratory to verify the correctness and completeness of the vendor’s rationale, then the vendor **shall not** make an IID claim for the noise source. (See SP 800-90B Section 3.1.2, Section 3.2.2 Requirement #5, IG 7.18). | Required | Validation Process. §2.1, §3.2, §4.3 |
| 101 | Resolution 3 | For Section 3.1.5, all processing of the raw data output from the noise sources that happens before it is ultimately output from the entropy source **shall** occur within a conditioning chain: a finite sequence of one or more conditioning components where each conditioning component in the chain receives any input data that is claimed to contain entropy from either the primary noise source (for the first conditioning component in the conditioning chain), or from the previous conditioning component in the conditioning chain (for all other conditioning components). | Required | §2.3, §6.3 and its subsections |
| 102 | Resolution 3 | An entropy estimate for the output of each conditioning component making up the conditioning chain **shall** be produced. | Required | §6, §6.3 and their subsections |
| 103 | Resolution 3 | For each non-vetted conditional component within a chain, an entropy estimate h', defined in Section 3.1.5.2, **shall** be computed using the statistical tests on the conditioned sequential data set for this component, as specified in Section 3.1.5.2. | Required | §6, §6.3 and their subsections |
| 104 | Resolution 3 | If claiming this property, it is the responsibility of the vendor and the testing lab to demonstrate that the mapping performed by the conditioning function is indeed bijective. They **shall** describe the set A of random data samples before conditioning, the set B of samples after the conditioning, and then show that the mapping of A to B performed by the conditioning function is both injective (the different elements of A map into the different elements of B) and surjective (every element of B has an element of A that maps into it.) | Required only for a bijective, non-vetted conditioning component. | §6.2, §6.3 and its subsections |
| 105 | Resolution 4 | For Section 3.1.5, for each conditioning component within the conditioning chain, the vendor **shall** specify: (a). the parameter n\_in, a lower bound for the amount of input data obtained from the primary noise source (for the first conditioning component) or the prior conditioning component in the chain (for all other conditioning components), and (b). the parameter h\_in, a lower bound for the assessed entropy supplied within this data. | Required | §6, §6.3 and their subsections |
| 106 | Resolution 5 | If a non-vetted conditioning component retains state and the primary noise source is non-independent, then the vendor **shall** provide mathematical evidence that the conditioning component’s entropy output is not below its assessed value (h\_out). | Required only for non-vetted conditioning components with state and where the primary noise source is not independent. | §3.2, §4.3, §6, §6.2, and their subsections  |
| 107 | Resolution 5 | This mathematical evidence **shall** justify why the reduction of the conditioning component’s output entropy due to the cancellation of mutual information present in both the data input to the conditioning component and the retained state does not result in the output entropy of the conditioning component being below its assessed value (h\_out). | Required only for non-vetted conditioning components with state and where the primary noise source is not independent. | §3.2, §4.3, §6.2 |
| 108 | Resolution 6 | The presence of supplemental data **shall not** be credited for the purpose of computing h\_in or n\_in. (See SP 800-90B Sections 3.1.5.1.2 and 3.1.6). | Required | §2.3, §6.3 and its subsections |
| 109 | Resolution 7 | For Section 3.1.5.1.1, in order for a conditioning function to qualify as “vetted”, it **shall** consist solely of one of the listed vetted functions in this section | Required only for vetted conditioning components. | §6, §6.3 and their subsections |
| 110 | Resolution 8 | For Section 3.1.5 and its subsections, nw **shall not** be claimed to be greater than n\_in.  | Required | §2.3, §6.3 and its subsections |
| 111 | Resolution 8 | The narrowest width for non-vetted conditioning components **shall** be established by analysis of their designs. | Required only for non-vetted conditioning components. | §2.3, §6.3 and its subsections |
| 112 | Resolution 8 | The tester **shall** describe how application of Appendix E resulted in the reported narrowest internal width (nw) values. | Required only for non-vetted conditioning components. | §2.3, §6.3 and its subsections |
| 113 | Resolution 9 | For Section 3.1.5, if the conditioning function can be shown to be bijective, then the vendor may claim that h\_out = h\_in. If this bijective conditioning function is non-vetted, then its output **shall** **not** be truncated, as per Section 3.1.5.2. | Required only for non-vetted conditioning components. | §2.3, §6.2, §6.3 and its subsections |
| 114 | Resolution 9 | Any transform that is reversible is bijective, and the tester **shall** specify a detailed procedure for reversing any conditioning function that is claimed to be bijective. | Required only for a bijective, non-vetted conditioning component. | §2.3, §6.2, §6.3 and its subsections |
| 115 | Resolution 10 | Combining the outputs of the noise source copies under this provision **shall** be considered part of the digitization process, and so Resolution #1 **shall** apply. | Required | §2.1, §3.2 |
| 116 | Resolution 13 | The technical argument supporting the expected H\_submitter value **shall** be based on the vendor’s description of the source of unpredictability within the noise source and how the noise source outputs vary depending on this identified unpredictability. | Required | §2.1, §3.2, §3.3 |
| 117 | Resolution 13 | Statistical testing may be used to establish parameters referenced within this argument, but the H\_submitter value **shall** **not** be the result of some general statistical testing process that does not account for the design of the noise source | Required | §3.2, §3.3 |
| 118 | Resolution 14 | If the design integrates the described RCT and APT tests and these tests are shown to not detect the vendor-identified known or suspected noise source failure modes, then the developer **shall** include additional developer-defined continuous testing that does detect the vendor-identified noise source failure modes (irrespective of Section 4.4’s statement that the RCT and APT are the only tests required). | Optional | §2.2; §5.2, §5.3 and their subsections |
| 119 | Resolution 14 | The tester **shall** verify that all the vendor-identified known or suspected noise source failure modes are detected by the continuous health tests included within the entropy source. (See SP 800-90B Section 4.3, Requirements #1, #7, #8 and #9). | Optional | §2.2; §5.2, §5.3 and their subsections |
| 120 | Resolution 15 | When stating the false positive rate (alpha) to satisfy the requirement, the false positive rate may be either the alpha used to generate the cutoffs for the APT/RCT tests or the actual observed false positive rate experienced by this health test when supplied with raw data from the noise source in use. The developer **shall** describe the exact meaning of the specified false positive rate and what the relation is between this false positive rate and any cutoff values used with the health tests | Optional when the value is within the recommended range in Requirement 70. Required when the value is outside of the recommended range in Requirement 70. | §5.2 and its subsections |
| 121 | Resolution 16 | For Section 4.4.2, the cutoff value C for the APT **shall** be no larger than the window size (i.e., C ≤ W). | Required | §2.2, §5.2 and its subsections |
| 122 | Resolution 17 | For such noise sources, H\_submitter and H = min(H\_r, H\_c , H\_i) in Sections 3.1.3 and 3.1.4.2 **shall** reflect an entropy bound that can be justified in the average case and/or on a per-symbol basis with high probability. | Required | §3.2, §4 and its subsections |
| 123 | Resolution 18 | For Section 4.5, when using simulation to argue that the developer-provided health test satisfies the requirements of Section 4.5, the developer **shall** specify how the data used within this simulation was created. | Required only for developer defined health tests. | §5.4 and its subsections |
| 124 | Resolution 18 | To fulfill the Section 4.5 requirements using simulation, at least 1 million rounds of simulation **shall** be used for each simulated health test, and there **shall** be sufficient simulation rounds so that at least five health test failures are observed for each health test. | Required only for developer defined health tests. | §5.4 and its subsections |
| 125 | Additional Comment 3 | The tester **shall** verify that each conditioning component’s implementation is fully consistent with the component’s design. This verification **shall** be performed by means of either running a computerized test developed for testing just the conditioning component (separate from the statistical testing of the noise source) or by the code review. The lab **shall** describe in the Entropy Test Report submitted to the CMVP the chosen method for verifying the correctness of each conditioning component’s implementation. | Required | The CST Laboratory must conduct this review. |

1. Modeling Calculations
2. Simulations

## Simulation Code

## Simulation Results

1. Glossary

## Notation Used

## Definitions

1. Data Gathering Procedures and Controls

## Data Gathering Procedures

<Describe who performed the data extraction, and the relevant circumstances. This data collection must be conducted either by the submitter with a witness from the testing lab (in this case, document who the witness was), by the testing lab itself, or prepared by the submitter in advance of testing.>

### Raw Data Acquisition Procedure

<This section must include a specification of the raw data acquisition procedure. This procedure must be sufficiently detailed to allow a lab or submitter to perform (or replicate) the collection process at a later time, if necessary.>

### Restart Data Acquisition Procedure

<This section must include a specification of the restart data acquisition procedure. This procedure must be sufficiently detailed to allow a lab or submitter to perform (or replicate) the collection process at a later time, if necessary.>

### Conditioned Data Acquisition Procedure

<If there is non-vetted conditioning, then for each non-vetted conditioning component, this section must include a specification of the conditioned data acquisition procedure for each non-vetted conditioning component. This procedure must be sufficiently detailed to allow a lab or submitter to perform (or replicate) the collection process at a later time, if necessary.>

## Vendor Attestation

<If the submitter prepared the data in advance of the testing, they must supply a signed document that attests that the specified procedure was used to produce the submitted datasets.>

<CMVP will provide an example form for this attestation.>

1. The $r$-stabilized assessments are generated using the [Theseus [non-iid-main](https://github.com/KeyPair-Consulting/Theseus/blob/master/src/non-iid-main.c)] tool, whose per-subset results are consistent with those produced by the NIST entropy evaluation tool. The LBA tests are conducted using the NIST test suite (GitHub commit 6bfed9fe238ab7f00895ceb603c7a5e55b61a5a2). [↑](#footnote-ref-2)
2. <Comment on the reason for specifying the reported level of precision.> [↑](#footnote-ref-3)
3. Per the Note in [NIST SHALL], the requirement should state: "The size of the conditioning component input **shall** at least be a multiple of the size of the noise source output, such that at least n\_in bits of whole samples are utilized." [↑](#footnote-ref-4)