Intel Digital Random Number Generator SP800-90B Non-Proprietary Public Use Document

Intel Entropy Source

May 2023

Revision 0.3.4

Intel Confidential

Document Number: 616000

Contents

Figures

Tables

Revision History

Revision Number	Description	Date
0.3.4	• Updates related to Federal Information Processing Standard (FIPS) 140-3 IG	May 2023
0.3.3	• Title update, CHIP name update.	April 2023
0.3.2	• Initial release of the document.	March 2023

1 Description

The Intel Entropy Source is a physical (P) entropy source.

The circuit component is RNG_ES_SKX_1.0

The synthesizable RTL component is SKX-COOP-RTL1.0

All components of the entropy source are hardware, consisting of logical and electronic components bounded in a rectangle of silicon. There is no firmware or software within the entropy source.

The entropic data from the entropy source is Non-IID.

This PUD is applicable to the following products:

Table 1-1. List of Applicable Devices

Processor Name	Processor Name
Intel® Xeon® Gold 5117 Processor	Intel® Xeon® Gold 6254 Processor
Intel® Xeon® Gold 5117F Processor	Intel® Xeon® Gold 6256 Processor
Intel® Xeon® Gold 5117M Processor	Intel® Xeon® Gold 6258R Processor
Intel® Xeon® Gold 5122 Processor	Intel® Xeon® Gold 6261 Processor
Intel® Xeon® Gold 5122M Processor	Intel® Xeon® Gold 6262 Processor
Intel® Xeon® Gold 5215 Processor	Intel® Xeon® Gold 6262V Processor
Intel® Xeon® Gold 5218 Processor	Intel® Xeon® Gold 6263CY Processor
Intel® Xeon® Gold 5218R Processor	Intel® Xeon® Gold 6264 Processor
Intel® Xeon® Gold 5218T Processor	Intel® Xeon® Gold 6266C Processor
Intel® Xeon® Gold 5219C Processor	Intel® Xeon® Gold 6267 Processor
Intel® Xeon® Gold 5219Y Processor	Intel® Xeon® Gold 6267C Processor
Intel® Xeon® Gold 5220 Processor	Intel® Xeon® Gold 6268CL Processor
Intel® Xeon® Gold 5220R Processor	Intel® Xeon® Gold 6268L Processor
Intel® Xeon® Gold 5220S Processor	Intel® Xeon® Gold 6269C Processor
Intel® Xeon® Gold 5220T Processor	Intel® Xeon® Gold 6269Y Processor
Intel® Xeon® Gold 5222 Processor	Intel® Xeon® Gold 6270 Processor
Intel® Xeon® Gold 5281C Processor	Intel® Xeon® Gold 6270C Processor
Intel® Xeon® Gold 6122 Processor	Intel® Xeon® Gold 6271 Processor
Intel® Xeon® Gold 6126 Processor	Intel® Xeon® Gold 6271C Processor
Intel® Xeon® Gold 6126F Processor	Intel® Xeon® Gold 6272 Processor
Intel® Xeon® Gold 6126FM Processor	Intel® Xeon® Gold 6273 Processor
Intel® Xeon® Gold 6126M Processor	Intel® Xeon® Gold 6273C Processor
Intel® Xeon® Gold 6126T Processor	Intel® Xeon® Gold 6278 Processor

Processor Name	Processor Name
Intel® Xeon® Gold 6126TM Processor	Intel® Xeon® Gold 6278C Processor
Intel® Xeon® Gold 6127 Processor	Intel® Xeon® Gold 6290 Processor
Intel® Xeon® Gold 6127M Processor	Intel® Xeon® Gold 6292 Processor
Intel® Xeon® Gold 6128 Processor	Intel® Xeon® Gold 6299C Processor
Intel® Xeon® Gold 6128M Processor	Intel® Xeon® Platinum 6164 Processor
Intel® Xeon® Gold 6130 Processor	Intel® Xeon® Platinum 8124 Processor
Intel® Xeon® Gold 6130F Processor	Intel® Xeon® Platinum 8124M Processor
Intel® Xeon® Gold 6130FM Processor	Intel® Xeon® Platinum 8149 Processor
Intel® Xeon® Gold 6130H Processor	Intel® Xeon® Platinum 8149M Processor
Intel® Xeon® Gold 6130M Processor	Intel® Xeon® Platinum 8151 Processor
Intel® Xeon® Gold 6130T Processor	Intel® Xeon® Platinum 8153 Processor
Intel® Xeon® Gold 6130TM Processor	Intel® Xeon® Platinum 8156 Processor
Intel® Xeon® Gold 6131 Processor	Intel® Xeon® Platinum 8156M Processor
Intel® Xeon® Gold 6132 Processor	Intel® Xeon® Platinum 8157 Processor
Intel® Xeon® Gold 6132M Processor	Intel® Xeon® Platinum 8157M Processor
Intel® Xeon® Gold 6133 Processor	Intel® Xeon® Platinum 8158 Processor
Intel® Xeon® Gold 6134 Processor	Intel® Xeon® Platinum 8158M Processor
Intel® Xeon® Gold 6134M Processor	Intel® Xeon® Platinum 8160 Processor
Intel® Xeon® Gold 6135 Processor	Intel® Xeon® Platinum 8160F Processor
Intel® Xeon® Gold 6135M Processor	Intel® Xeon® Platinum 8160FM Processor
Intel® Xeon® Gold 6136 Processor	Intel® Xeon® Platinum 8160H Processor
Intel® Xeon® Gold 6136M Processor	Intel® Xeon® Platinum 8160M Processor
Intel® Xeon® Gold 6137 Processor	Intel® Xeon® Platinum 8160T Processor
Intel® Xeon® Gold 6137M Processor	Intel® Xeon® Platinum 8160TM Processor
Intel® Xeon® Gold 6138 Processor	Intel® Xeon® Platinum 8162 Processor
Intel® Xeon® Gold 6138F Processor	Intel® Xeon® Platinum 8163 Processor
Intel® Xeon® Gold 6138M Processor	Intel® Xeon® Platinum 8164 Processor
Intel® Xeon® Gold 6138P Processor	Intel® Xeon® Platinum 8164M Processor
Intel® Xeon® Gold 6138T Processor	Intel® Xeon® Platinum 8165 Processor
Intel® Xeon® Gold 6138TM Processor	Intel® Xeon® Platinum 8165M Processor
Intel® Xeon® Gold 6139 Processor	Intel® Xeon® Platinum 8166 Processor
Intel® Xeon® Gold 6139M Processor	Intel® Xeon® Platinum 8167M Processor
Intel® Xeon® Gold 6140 Processor	Intel® Xeon® Platinum 8168 Processor
Intel® Xeon® Gold 6140F Processor	Intel® Xeon® Platinum 8168F Processor
Intel® Xeon® Gold 6140FM Processor	Intel® Xeon® Platinum 8168FM Processor
Intel® Xeon® Gold 6140M Processor	Intel® Xeon® Platinum 8168M Processor

Processor Name	Processor Name
Intel® Xeon® Gold 6141 Processor	Intel® Xeon® Platinum 8170 Processor
Intel® Xeon® Gold 6141M Processor	Intel® Xeon® Platinum 8170M Processor
Intel® Xeon® Gold 6142 Processor	Intel® Xeon® Platinum 8171 Processor
Intel® Xeon® Gold 6142F Processor	Intel® Xeon® Platinum 8171M Processor
Intel® Xeon® Gold 6142FM Processor	Intel® Xeon® Platinum 8172M Processor
Intel® Xeon® Gold 6142M Processor	Intel® Xeon® Platinum 8173M Processor
Intel® Xeon® Gold 6143 Processor	Intel® Xeon® Platinum 8174 Processor
Intel® Xeon® Gold 6143M Processor	Intel® Xeon® Platinum 8175M Processor
Intel® Xeon® Gold 6144 Processor	Intel® Xeon® Platinum 8176 Processor
Intel® Xeon® Gold 6144M Processor	Intel® Xeon® Platinum 8176F Processor
Intel® Xeon® Gold 6145 Processor	Intel® Xeon® Platinum 8176FM Processor
Intel® Xeon® Gold 6145M Processor	Intel® Xeon® Platinum 8176M Processor
Intel® Xeon® Gold 6146 Processor	Intel® Xeon® Platinum 8177 Processor
Intel® Xeon® Gold 6146M Processor	Intel® Xeon® Platinum 8177M Processor
Intel® Xeon® Gold 6147 Processor	Intel® Xeon® Platinum 8179M Processor
Intel® Xeon® Gold 6147M Processor	Intel® Xeon® Platinum 8180 Processor
Intel® Xeon® Gold 6148 Processor	Intel® Xeon® Platinum 8180M Processor
Intel® Xeon® Gold 6148F Processor	Intel® Xeon® Platinum 8201 Processor
Intel® Xeon® Gold 6148M Processor	Intel® Xeon® Platinum 8222CL Processor
Intel® Xeon® Gold 6149 Processor	Intel® Xeon® Platinum 8222L Processor
Intel® Xeon® Gold 6150 Processor	Intel® Xeon® Platinum 8223CL Processor
Intel® Xeon® Gold 6150F Processor	Intel® Xeon® Platinum 8224CL Processor
Intel® Xeon® Gold 6150FM Processor	Intel® Xeon® Platinum 8224L Processor
Intel® Xeon® Gold 6150M Processor	Intel® Xeon® Platinum 8247C Processor
Intel® Xeon® Gold 6151 Processor	Intel® Xeon® Platinum 8249C Processor
Intel® Xeon® Gold 6151M Processor	Intel® Xeon® Platinum 8251 Processor
Intel® Xeon® Gold 6152 Processor	Intel® Xeon® Platinum 8251C Processor
Intel® Xeon® Gold 6152M Processor	Intel® Xeon® Platinum 8252C Processor
Intel® Xeon® Gold 6154 Processor	Intel® Xeon® Platinum 8253 Processor
Intel® Xeon® Gold 6154M Processor	Intel® Xeon® Platinum 8255C Processor
Intel® Xeon® Gold 6155 Processor	Intel® Xeon® Platinum 8256 Processor
Intel® Xeon® Gold 6155M Processor	Intel® Xeon® Platinum 8257 Processor
Intel® Xeon® Gold 6159 Processor	Intel® Xeon® Platinum 8259CL Processor
Intel® Xeon® Gold 6159M Processor	Intel® Xeon® Platinum 8259L Processor
Intel® Xeon® Gold 6161 Processor	Intel® Xeon® Platinum 8260 Processor
Intel® Xeon® Gold 6161M Processor	Intel® Xeon® Platinum 8260AS Processor
Intel® Xeon® Gold 6162 Processor	Intel® Xeon® Platinum 8260C Processor

Processor Name	Processor Name
Intel® Xeon® Gold 6208U Processor	Intel® Xeon® Platinum 8260L Processor
Intel® Xeon® Gold 6209U Processor	Intel® Xeon® Platinum 8260M Processor
Intel® Xeon® Gold 6210U Processor	Intel® Xeon® Platinum 8260Y Processor
Intel® Xeon® Gold 6212U Processor	Intel® Xeon® Platinum 8263C Processor
Intel® Xeon® Gold 6222 Processor	Intel® Xeon® Platinum 8264 Processor
Intel® Xeon® Gold 6222V Processor	Intel® Xeon® Platinum 8265 Processor
Intel® Xeon® Gold 6226 Processor	Intel® Xeon® Platinum 8268 Processor
Intel® Xeon® Gold 6226R Processor	Intel® Xeon® Platinum 8269C Processor
Intel® Xeon® Gold 6230 Processor	Intel® Xeon® Platinum 8269CL Processor
Intel® Xeon® Gold 6230N Processor	Intel® Xeon® Platinum 8269CY Processor
Intel® Xeon® Gold 6230R Processor	Intel® Xeon® Platinum 8270 Processor
Intel® Xeon® Gold 6230T Processor	Intel® Xeon® Platinum 8270CL Processor
Intel® Xeon® Gold 6231 Processor	Intel® Xeon® Platinum 8271CL Processor
Intel® Xeon® Gold 6231C Processor	Intel® Xeon® Platinum 8271L Processor
Intel® Xeon® Gold 6233 Processor	Intel® Xeon® Platinum 8272CL Processor
Intel® Xeon® Gold 6234 Processor	Intel® Xeon® Platinum 8272L Processor
Intel® Xeon® Gold 6235 Processor	Intel® Xeon® Platinum 8273CL Processor
Intel® Xeon® Gold 6238 Processor	Intel® Xeon® Platinum 8273L Processor
Intel® Xeon® Gold 6238L Processor	Intel® Xeon® Platinum 8274 Processor
Intel® Xeon® Gold 6238M Processor	Intel® Xeon® Platinum 8275CL Processor
Intel® Xeon® Gold 6238R Processor	Intel® Xeon® Platinum 8275L Processor
Intel® Xeon® Gold 6238T Processor	Intel® Xeon® Platinum 8276 Processor
Intel® Xeon® Gold 6240 Processor	Intel® Xeon® Platinum 8276AS Processor
Intel® Xeon® Gold 6240C Processor	Intel® Xeon® Platinum 8276CL Processor
Intel® Xeon® Gold 6240L Processor	Intel® Xeon® Platinum 8276L Processor
Intel® Xeon® Gold 6240M Processor	Intel® Xeon® Platinum 8276M Processor
Intel® Xeon® Gold 6240R Processor	Intel® Xeon® Platinum 8277L Processor
Intel® Xeon® Gold 6240Y Processor	Intel® Xeon® Platinum 8280 Processor
Intel® Xeon® Gold 6241C Processor	Intel® Xeon® Platinum 8280AS Processor
Intel® Xeon® Gold 6241CM Processor	Intel® Xeon® Platinum 8280L Processor
Intel® Xeon® Gold 6241L Processor	Intel® Xeon® Platinum 8280M Processor
Intel® Xeon® Gold 6242 Processor	Intel® Xeon® Platinum 8284 Processor
Intel® Xeon® Gold 6242R Processor	Intel® Xeon® Platinum P-8124 Processor
Intel® Xeon® Gold 6243 Processor	Intel® Xeon® Platinum P-8136 Processor
Intel® Xeon® Gold 6244 Processor	Intel® Xeon® W-3175X Processor
Intel® Xeon® Gold 6246 Processor	Intel® Xeon® W-3223 Processor
Intel® Xeon® Gold 6246R Processor	Intel® Xeon® W-3225 Processor

Processor Name	Processor Name
Intel® Xeon® Gold 6248 Processor	Intel® Xeon® W-3235 Processor
Intel® Xeon® Gold 6248R Processor	Intel® Xeon® W-3245 Processor
Intel® Xeon® Gold 6250 Processor	Intel® Xeon® W-3245M Processor
Intel® Xeon® Gold 6250L Processor	Intel® Xeon® W-3265 Processor
Intel® Xeon® Gold 6252 Processor	Intel® Xeon® W-3265M Processor
Intel® Xeon® Gold 6252N Processor	Intel® Xeon® W-3275 Processor
Intel® Xeon® Gold 6253CL Processor	Intel® Xeon® W-3275M Processor
Intel® Xeon® Gold 6253L Processor	

2 Security Boundary

The entropy source security boundary surrounds the set of components referred to as the Digital Random Number Generator (DRNG) core, that includes the noise source, digitizer, Continuous Health Tests (CHT), AES-CBC-MAC Vetted Conditioning Component, Deterministic Random Bit Generator (DRBG), Non-deterministic Random Bit Generator (NRBG) and register interface.

For use as a full entropy source, the NRBG output of the DRNG is the necessary output. This is accessed through the Intel CPU instruction “RdSeed”.

The security boundary is a sub boundary within the DRNG. Components outside the security boundary but within the DRNG are to attach to the local bus, clock and power systems on the chip.

The DRNG security boundary is not a Federal Information Processing Standard (FIPS) 140 security boundary. It is designed to be usable within a larger FIPS 140 security boundary through compliance to SP800-90Arev1, B and draft C along with relevant requirements in ISO/IEC 19790-2012 and FIPS 140-3.

The bold outline in Figure 2-1 shows the security boundary of the entropy source and other RNG components.

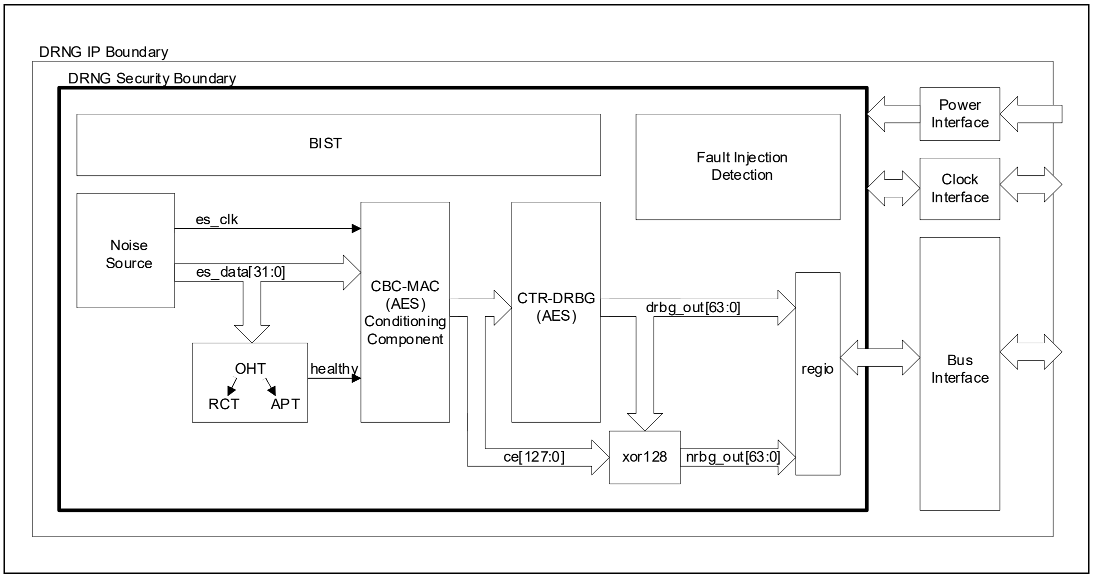
The NRBG output path to the region block is the output of the full entropy source, as an RBG3 construction.

The DRBG output path to the region block is the output of the DRBG, as an RBG2 construction.

The NRBG construction is the XOR (RBG3) construction NRBG from Draft SP800-90C. This XORs the output of the conditioner with an output from the DRBG to form the NRBG output. The strength of the XOR is entirely dependent on the full entropy of the conditioner output. The DRBG’s input into the XOR, as well as the XOR operation itself are not considered part of the conditioning chain.

The width of these operations is 128 bits, driven by the output size of AES. The registers sizes are 64 bits and in the logic, this width transforming is performed using a FIFO that is 64 bits wide and takes in 128 bits as two 64-bit entries and outputs 64 bits to match the register width.

Figure 2-1. DRBG Security Boundary



In the context of an Intel CPU, the DRNG register that presents the NRBG output to the local bus is called `egetdata`. This register is read by the CPU whenever the `RdSeed` instruction is executed. The result is passed to the target register of the instruction and the success or failure signaled in the carry flag.

This report is applicable to the devices in Table 1-1. The silicon manufacturing process, IC design and DRNG design is identical for each of these devices. Differences between these devices are the set of enabled features, which has no influence on the RNG behavior.

3 Operating Conditions

The entropy source is guaranteed to operate within the designated operating envelope in the data sheet of the chip. In **Intel® Xeon® Platinum 8176 Processor** the operating envelope is as follows:

Table 3-1. Operating Conditions

Parameter	Minimum	Maximum
Temperature	0 °C	89 °C

These conditions are taken from the Intel Automated Relational Knowledge-Base (ARK) specifications:

https://www.intel.com/content/www/us/en/products/sku/120508/intel-xeon-platinum-8176-processor-38-5m-cache-2-10-ghz/specifications.html

4 Configuration Settings

There are no configuration settings accessible at any privilege level to software running in the CPU.

5 Physical Security Mechanisms

The RNG contains a security boundary described in Section 2. In the operating mode of the RNG, there is hardware enforcement of the security of the boundary.

Specifically:

- Diagnostic output of raw data from the boundary is disabled.
- Debugging port access to internal state of the RNG is disabled at the boundary.
- Configuration input written to registers is ignored and the default configuration is enforced.
- Algorithms are implemented to detect stuck output failures.
- Register write privileges are enforced in hardware.

When an alarm is triggered, the RNG resets itself and re-runs Built-In Self-Test (BIST). It is not possible to distinguish between a failure due to attack or environmental bounds violation or a rare false positive error. The re-running of BIST will lead to the RNG failing if the BIST fails. In the case of a transitory error, the RNG will recover when BIST is re-run.

The packaging of the chip is a tamper evident enclosure.

6 Conceptual Interfaces

For consuming applications running in software on the CPU, `GetEntropy(n)` is implemented by the `RdSeed` instruction, where *n* can be one of 16, 32 or 64, depending on the size of the target register.

Internally to the security boundary, for feeding conditioner output data to the DRBG, `Get_entropy()` is implemented in digital logic between the conditioner and DRBG in the form of a 128-bit wide First In, First Out (FIFO).

7 Min Entropy Rate

The assessed entropy from the noise source, as per Section 3.1.4.2 of the SP800-90B, is *min(Hr, Hc, HI) = 0.6 bits* of entropy per bit of data.

H_{out} from the CBC-MAC conditioning component, assessed according to Section 3.1.5 of the SP800-90B, is *1-ε where ε << 2-32*, meeting the draft requirement for full entropy in draft SP800-90C.

The assessment of the conditioner output entropy is computed with the lower bound of the conditioner input data set above the CHT pass threshold of 0.6, the conditioner entropy output assessed using the equations in SP800-90B, Section 3.1.5.1.2, are:

```
H_out = Output_Entropy(n_in, n_out, nw, h_in) where
 n_in   = 512
 n_out  = 128
 nw     = 128
 h_in = 0.6 * 512 = 307.2
```

When using a conditioning component listed in Section 3.1.5.1.1 (given the assurance of correct implementation by Cryptographic Algorithm Validation Program (CAVP) testing), the entropy of the output is estimated as:

$$h_{out} = Output\_Entropy(n_{in}, n_{out}, nw, h_{in})$$

Where $Output\_Entropy(n_{in}, n_{out}, nw, h_{in})$ is described as follows:

1. Let $P_{high} = 2^{-h_{in}}$ and $P_{low} = \frac{(1-P_{high})}{2^{n_{in}-1}}$.
2. N = min(n_{out},nw).
3. $\Psi = 2^{n_{in}-n} P_{low} + P_{high}$
4. $U = 2^{n_{in}-n} + \sqrt{2n(2^{n_{in}-n})In(2)}$
5. $\Omega = U \times P_{low}$
6. Return – $\log_2(\max(\psi,\omega))$

This was evaluated using 1,000 binary digit floating point arithmetic.

```
#!/usr/bin/env python3

from __future__ import print_function

import UsrIntel.R1 # Intel specific import to get the standard libraries
import math
from mpmath import *

PRECISION = 1000 # 1,000  of precision.
```

```
def output_entropy(n_in,n_out,nw, h_in):
    n = min(n_out,nw)
    ttninmn = mpf(2.0)**(n_in-n)
    p_high = mpf(2.0)**(-h_in)
    p_low = (mpf(1.0)-p_high)/((mpf(2.0)**n_in)-mpf(1.0))
    phi = ttninmn*p_low + p_high
    U = ttninmn + sqrt(mpf(2.0) * n * ttninmn * log(mpf(2.0)))
    w = U * p_low
    return -log(max(phi,w),2)

if __name__=="__main__":
    mp.prec = PRECISION
    entropy_rate = 0.6
    n_in = 512
    h_in = n_in*entropy_rate

    entropy = output_entropy(mpf(n_in), mpf(128.0), mpf(128.0), mpf(h_in))
    epsilon = mpf(128.0)-entropy

    # compute human readable epsilon
    for i in range(1,1024):
        power = mpf(i)
        ne = epsilon*(2**power)
        if ne > 1:
            print("epsilon = %s*2^-%d" % (nstr(ne,8),i))
            break

> ./pud_entropy.py
epsilon = 1.255939*2^-179
```

The result shows the lower bound of epsilon for entropy rates above the pass threshold of the CHT is, to four digits of precision $1.255*2^{-179}$, which meets the requirement for epsilon the be less than 2^{-32}.

8 Health Tests

The DRNG includes:

- Continuous Health Tests (CHT).
- Startup Noise Source Health Tests.
- Startup Logic Integrity BIST.

The CHT is composed of a short-term test yielding a pass/fail over individual 256-bit blocks of noise source data, and a long-term evaluation of the pass/fail history of the past 256 blocks (totaling 65536 bits) to infer an entropy source failure. The failure condition is invoked when the pass/fail rate drops below 50%.

The logic integrity test is one of the startup tests. This performs a test of the digital logic by running deterministic random sequences through all the logic and testing the resulting output against the expected result.

The Startup Noise Source Health Test involves running the CHT for a probationary period of 65536 bits from the noise source. When the test is complete, assuming the test passes, the RNG enters the operational state. This happens during CPU startup and completes before the first CPU instructions can execute. Thus, `RdSeed` is available from initial instruction execution time.

The startup test is invoked at power-on or exiting the reset state. Thus, the startup tests can be invoked by power cycling the CPU or resetting the CPU.

A failure any of the startup tests (logic integrity or noise source health test) will be reflected as a BIST failure in the internal status register which leads to an MCHECK failure of the CPU.

Following the startup tests, the CHT continue to run. Should failure condition of the CHT test be encountered after the startup tests have completes, this may be either the result of a soft error or a hard error. The test will continue to run and should the entropy quality return, it will exit the failure state. In the failure state, no more random numbers are issued, and the failure state is reflected in the internal state registers, which is visible at the instruction interface by the repeated failure to deliver random numbers, through the returned carry flag of the `RdRand` and `RdSeed` instructions being 0.

A sequence of 1000 back-to-back 0 carry flags on `RdSeed` can be inferred to be an error. Should some condition exist (for example, out of specification operating condition), cessation of that condition will lead to resumption of the supply of random numbers.

A less computationally expensive test of failure is the response from the `RdRand` instruction (not a noise source output, but an RBG2 output), which due to its higher output rate has a 0% chance of underflows arising from high consumption demand by other threads, and so 10 back-to-back failures are specified as a runtime error.

9 Maintenance

There are no maintenance action requirements.

10 Required Testing

We performed raw noise testing using the non-IID lower bound entropy tests of the SP800-90B Entropy Assessment software tool, showing the entropy from the noise source to exceed the minimum input threshold of 0.299 of the vetted conditioning components.

We performed restart testing using the SP800-90B Entropy Assessment software tool, showing the startup min entropy of *Hr* and *Hc* to be greater than 50% of *HI*.