SP 800-90B NON-PROPRIETARY PUBLIC USE DOCUMENT

INFOBLOX NIOS 9.0.7'S CPU JITTER RNG 3.6.2

DOCUMENT VERSION: 1.0

DATE: AUGUST 26, 2026

Prepared by:



Leidos Inc.
www.leidos.com/commercialcyber/ate
Leidos Accredited Testing & Evaluation (AT&E) Lab
6841 Benjamin Franklin Drive, Columbia, MD 21046

Prepared for:



Infoblox
https://www.infoblox.com/
2390 Mission College BLVD, Suite 501
Santa Clara, CA 95054
USA

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

Document Version History		
Version	**Date**	**Change**
1.0	8/26/2026	Initial validation

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

Table of Contents

1. DESCRIPTION 4
2. SECURITY BOUNDARY 5
3. OPERATING CONDITIONS 6
4. CONFIGURATION SETTING 7
5. CONCEPTUAL INTERFACES 7
6. MIN-ENTROPY RATE 8
7. HEALTH TESTS 8
8. MAINTENANCE 9
9. USER VERIFICATION 9

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

1. DESCRIPTION

The entropy source for the Infoblox Trinzic Virtual Appliances and Trinzic Hardware Appliances running the Network Identity Operating System (NIOS) 9.0.7 is a software and non-physical (NP) implementation of the CPU Jitter RNG version 3.6.2. The Infoblox's CPU Jitter RNG 3.6.2 on NIOS 9.0.7 (hereafter referred to as "the Entropy Source") is not claimed to be IID and meets all the relevant non-IID standards of NIST SP 800-90B (version January 2018) and FIPS 140-3 IGs D.J, D.K, and D.O (version January 29, 2024). The Entropy Source was tested on 10 operational environments (OE)s listed in Table 1.

Table 1. Tested Operational Environments

OE Number	Processor	Osr values	Hypervisor	Operating System (OS)
1	Intel Xeon E5-2620v4 (Broadwell)	4	N/A	Network Identity Operating System (NIOS) 9.0.7
2	Intel Xeon E3-1275v5 (Skylake)	3		
3	Intel Xeon 6226R (Cascade Lake)	6		
4	Intel Xeon 4210R (Cascade Lake)	5		
5	Intel Xeon E-2334 (Rocket Lake)	10		
6	Intel Xeon E-2386G (Rocket Lake)	11		
7	Intel Xeon E-2388G (Rocket Lake)	11		
8	Intel(R) Xeon(R) Gold 6448H (Sapphire Rapids)	5	VMware ESXi 8.0	
9	Intel(R) Xeon(R) Platinum 8276 (Cascade Lake)	5		
10	Intel(R) Xeon(R) Gold 6248R (Cascade Lake)	9		

The following VM configurations were applied to the VMWare ESXi 8.0 hypervisor OE's.

- Hyperthreading (SMT): Enabled
- Power management policy: Balanced (dynamic) — not locked to static/max-performance; ACPI C-states enabled when idle; Performance/Energy Bias set to the Balanced preset
- vCPU pinning/affinity: No pinning configured on any VM — default ESXi CPU scheduler is used
- SMT/hyperthreading sharing: vCPUs are not isolated to dedicated physical cores; sibling logical threads may be shared with other VMs under the default scheduler
- Guest timer/TSC configuration: Default virtualized clock — no TSC passthrough or override configured on any VM
- CPU feature exposure: Each guest sees its host's native, unmasked CPU instruction/timing feature set

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

The entropy source is delivered as part of the NIOS firmware image, which supports the additional installation of a single hotfix per configuration. Use of the validated version of the Entropy Source is verified via the NIOS CLI “Show Version” command with the following values:

NIOS Version	Hotfix version
9.0.7-53931-516906214e77	Hotfix-9.0.7_J109839_APPLY-2fef2a55e53ab364f835f86e15091e28-Thu-Jul-2-09-19-08-2026.bin
	Hotfix-9.0.7_J109973_APPLY-61abb74ed5a4feea19ed842bebbc8c0f-Sun-May-3-17-02-35-2026.bin

2. SECURITY BOUNDARY

The Entropy Source is built from the jitterentropy-library version 3.6.2, IB_PRNG executable, and the NIOS Cryptographic Library, which operate within a defined security boundary that includes both software and hardware components. Specifically, the software components are the jitterentropy-library, IB_PRNG executable, and NIOS Cryptographic Library, and the relevant hardware component includes the memory, system timer and CPU of the underlying computational environment listed in Table 1.

Figure 1 depicts the overall design of the entropy source, which comprises the components that map to the conceptual components of an SP 800-90B compliant entropy source:

*A **primary noise source** whose randomness is accumulated by the timing variations (“Time Delta”) caused by memory accesses and execution time of a defined set of instructions outlined in the “Noise Source” box of*

- Figure 1
- **Health tests** component performed on the raw noise data to ensure the proper functioning of the entropy source
- A SHA3-256 vetted **conditioning component** (CAVP Cert. #A8012).
- A 2048 byte FIFO
- An AES-256 Counter DRBG with derivation function and prediction resistance enabled vetted **conditioning component** (CAVP Cert. #A8326)**.**

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

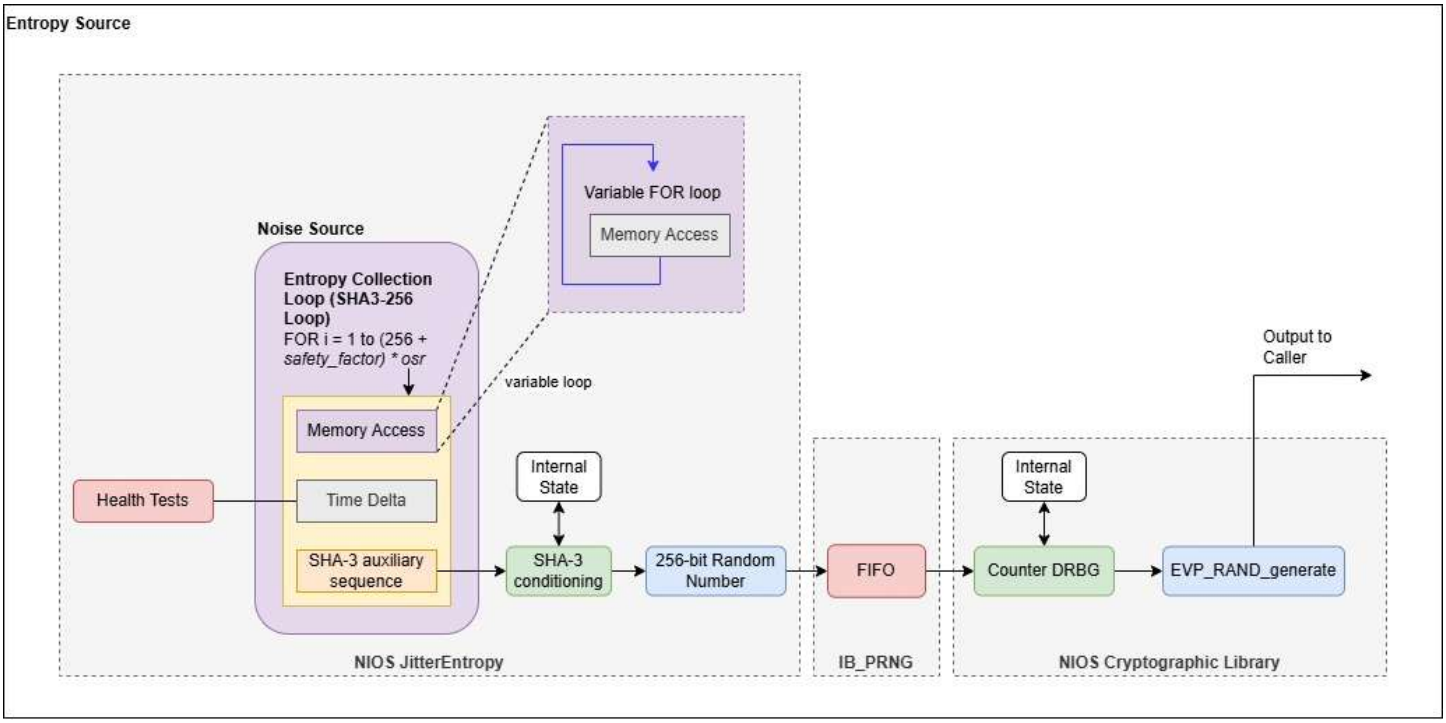


Figure 1. Entropy Source Design

3. OPERATING CONDITIONS

The Entropy Source is non-physical, and thus its operating conditions are inherited from the operational environment in which the entropy source is installed, as shown in Table 2 below.

Table 2. Operating Conditions across Operational Environments

OE Number	Processor					Hardware Platform	
	Name	Temperature Range	Voltage Range	Clock Speed	Cache Sizes	Temperature Range	Voltage Range (AC)
1	Intel Xeon E5-2620v4 (Broadwell)	$0℃ - 85\ ℃$	$0.65\ V - 1.45\ V$	$2.1\ GHz$	L1: 512 KB L2: 2 MB L3: 20 MB	$5℃ - 35\ ℃$	$100 - 240\ VAC$
2	Intel Xeon E3-1275v5 (Skylake)	$0℃ - 100\ ℃$	$0.55\ V - 1.52\ V$	$3.8\ GHz$	L1: 256 KB L2: 1 MB L3: 8 MB	$5℃ - 35\ ℃$	$100 - 240\ VAC$
3	Intel Xeon Gold 6226R (Cascade Lake)	$0℃ - 85\ ℃$	$0.6\ V - 1.35\ V$	$2.9\ GHz$	L1: 1 MB L2: 4 MB L3: 22 MB	$10℃ - 35\ ℃$	$100 - 240\ VAC$
4	Intel Xeon 4210R (Cascade Lake)	$0℃ - 85\ ℃$	$0.6\ V - 1.35\ V$	$2.4\ GHz$	L1: 640 KB L2: 2.5 MB L3: 13.75 MB	$5℃ - 35\ ℃$	$100 - 240\ VAC$

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

5	Intel Xeon E-2334 (Rocket Lake)	$0℃ - 100\ ℃$	$0.6\ V - 1.35\ V$	$3.4\ GHz$	L1: 512 KB L2: 2 MB L3: 8 MB	$5℃ - 35\ ℃$	$100 - 240\ VAC$
6	Intel Xeon E-2386G (Rocket Lake)	$0℃ - 100\ ℃$	$0.6\ V - 1.35\ V$	$3.5\ GHz$	L1: 480 KB L2: 3 MB L3: 12 MB	$5℃ - 35\ ℃$	$100 - 240\ VAC$
7	Intel Xeon E-2388G (Rocket Lake)	$0℃ - 100\ ℃$	$0.6\ V - 1.35\ V$	$3.2\ GHz$	L1: 640 KB L2: 4 MB L3: 16 MB	$5℃ - 35\ ℃$	$100 - 240\ VAC$
8	Intel(R) Xeon(R) Gold 6448H (Sapphire Rapids)	$0℃ - 83\ ℃$	$0.6\ V - 1.35\ V$	$2.4\ GHz$	L1: 2.56 MB L2: 64 MB L3: 60 MB	$10℃ - 35\ ℃$	$200 - 240\ VAC$
9	Intel(R) Xeon(R) Platinum 8276 (Cascade Lake)	$0℃ - 89\ ℃$	$0.7\ V - 1.3\ V$	$2.2\ GHz$	L1: 1.75 MB L2: 28 MB L3: 39 MB	$10℃ - 35\ ℃$	$200 - 240\ VAC$
10	Intel(R) Xeon(R) Gold 6248R (Cascade Lake)	$0℃ - 85\ ℃$	$0.6\ V - 1.3\ V$	$3\ GHz$	L1: 1536 KB L2: 24 MB L3: 35.75 MB	$10℃ - 35\ ℃$	$100 - 240\ VAC$

4. CONFIGURATION SETTING

The Entropy Source's configuration parameters are listed in Table 3. These values are finalized in Infoblox's implementation for NIOS 9.0.7 across all applications and cannot be modified or provided by a user.

Table 3. CPU Jitter Configuration Parameters

Parameter Number	Parameter	Default Value
1	JENT_CONF_DISABLE_LOOP_SHUFFLE	Defined
2	JENT_HEALTH_LAG_PREDICTOR	Defined
3	JENT_RANDOM_MEMACCESS	Defined
4	ENTROPY_SAFETY_FACTOR	64
5	JENT_MIN_OSR	3
6	JENT_MEMORY_SIZE	2^{17}
7	JENT_MEMORY_BITS	17
8	JENT_MEMORY_ACCESSLOOPS	128
9	JENT_CONF_ENABLE_INTERNAL_TIMER	Not Defined

5. CONCEPTUAL INTERFACES

The CPU Jitter RNG 3.6.2 on NIOS 9.0.7 provides the following interfaces:

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

- The **GetEntropy** interface is the EVP_RAND_generate() function, which takes in the number of bytes of entropy data requested as input, and generates the requested random bit stream and returns it to the caller.
- The **GetNoise** interface is the jent_measure_jitter() function, which is only available for validation purposes and not accessible by the user.
- The **HealthTest** interface is the jent_entropy_init_ex() function, which initializes the entropy source by passing in the corresponding osr values listed in Table 1 and performs the Health Tests outlined in Section 7.

6. MIN-ENTROPY RATE

The Entropy Source v3.6.2 provides 256 bits of min-entropy per 256-bit output.

7. HEALTH TESTS

The health tests, implemented in the Infoblox's CPU Jitter RNG 3.6.2 on NIOS 9.0.7, include the SP 800-90B's Continuous, Start-up, and On-Demand tests:

- The Continuous health tests consist of:
  - Stuck Test
  - Enhanced Repetition Count Test (RCT)
  - Adaptive Proportion Test (APT)
  - Lag Predictor Test
- The Start-up tests perform the entire set of Continuous heath tests on the first 1024 samples upon start-up, after the first 100 initial samples were tested for architectural failure modes.
- The On-Demand tests, which are essentially the Start-up tests, are triggered upon the current Entropy Source instance's deallocation and a new Entropy Source instance's allocation.

The outputs and meanings of the HealthTest interface in Section 5 are summarized in Table 4.

Table 4. Health Test Indicators

Output Code Value	Indication	Recovery Method
0	The Entropy Source is successfully initialized and passed Start-up Health Tests.	N/A
-1	The entropy collector is NULL.	Deallocate the current Entropy Source instance and reallocate new instance.
-2	The noise source fails the RCT.	
-3	The noise source fails the APT.	
-4	The timer cannot be initialized.	
-5	The noise source fails the Lag Predictor Test.	

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.

8. MAINTENANCE

For Infoblox CPU Jitter RNG 3.6.2 on NIOS 9.0.7, there is no special maintenance required to guarantee its min-entropy rate or performance.

9. USER VERIFICATION

The Entropy Source does not provide an operator-accessible mechanism for outputting raw samples. No testing other than the implemented health tests is required for obtaining assurance that the entropy source is operating correctly.

THIS DOCUMENT MAY FREELY BE REPRODUCED AND DISTRIBUTED IN ITS ORIGINAL ENTIRETY, WITHOUT REVISION.