2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

February 28, 2020

Whom It May Concern:

Acumen Security verified that the following software faithfully enforces the use of FIPS approved algorithms within,

Cisco Prime Infrastructure version 3.8.

The software version is known to operate on the following platform(s):

- GEN2 Appliance (PID: PI-UCS-APL-K9)
- GEN3 Appliance (PIDs: PI-UCSM5-APL-K9 & PI-UCSM5-APL-U-K9)
- DNAC appliance (PIDs: DN1-HW-APL & DN2-HW-APL)

Acumen Security confirmed that the following features leverage FIPS approved algorithms for operation,

Feature	**Cryptographic Service**
SNMPv3	• Session establishment supporting each service, • All underlying cryptographic algorithms supporting each services' key derivation functions, • Hashing for each service, • Symmetric encryption for each service.
SSH	
TLS(HTTPS)	

During the course of the review, Acumen Security confirmed that Cisco Prime Infrastructure version 3.8 uses FIPS Approved algorithms for the services that are listed in the table above.

To be more precise the module implements the CiscoSSL FOM 7.0a Cryptographic Library with FIPS_mode flag set to false. Acumen Security confirmed that the module implements FED_MODE that requires the FIPS Approved algorithms and key sizes to be used, these algorithms are CAVP tested and their use is hard coded in the module.

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

Ashit Vora
Laboratory Director