November 29, 2016

To Whom It May Concern:

Acumen Security verified that the following software faithfully embeds a FIPS 140-2 validated cryptographic module,

- NX-OS (v7.0)

The software is known to operate on the following platforms:

- Nexus 3000 Series Switches

During the course of the review, Acumen Security confirmed that the following FIPS 140-2 cryptographic module is incorporated into the product,

- CiscoSSL FIPS Object Module Version: 4.1, FIPS 140-2 certificate #2100

Acumen Security confirmed that the following features leverage the embedded module to provide cryptographic services,

- Encryption associated with the following services:
    - SSH,
    - SNMPv3,
    - RADIUS,
    - TACACS+.
- Hashing associated with the following services:
    - SSH,
    - SNMPv3,
    - RADIUS,
    - TACACS+.
- Key Derivation associated with the following services,
    - SSH,
    - SNMPv3.
- Diffie Hellman and Asymmetric Encryption associated with the following services,
    - SSH.

Additionally, Acumen Security confirmed that the above referenced cryptographic module is initialized in a manner consistent with the instructions provided in the non-proprietary Security Policy.

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