SAIC
From Science to Solutions

January 22, 2013

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

To Whom It May Concern:

SAIC completed its conformance review of the Cisco Systems, Inc.'s **Cisco Nexus 5000 Series Switches on NX-OS 5.2(1)** (the "Product") on January 22, 2013; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

1. OpenSSL FIPS Object Module v1.2 (FIPS 140-2 Cert. #1051)

Specifically, SAIC's review confirmed that:

1. Each of the integrated cryptographic modules (mentioned above) are initialized in a manner that is compliant with their individual security policies.

2. All cryptographic algorithms used for SSH v2 and SNMP v3 used for session establishment, are offloaded to OpenSSL FIPS Object Module v1.2 with FIPS 140-2 Cert. #1051

3. Bulk data encryption (via SSH v2 and SNMP v3) for the established SSH and SNMP secure connection uses the OpenSSL FIPS Object Module v1.2 with FIPS 140-2 Cert. #1051.

Details of SAIC's review, which consisted of source code review and operational testing, can be found in the attached test plan.

Please note that for this review, SAIC only examined the Product features referenced above and while the Product may contain other features or functionality, SAIC did not examine these during its review and makes no claims or representations regarding them. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed SAIC's analysis, testing, or results.

The intention of this letter is to provide independent opinion that the Product correctly integrates and uses validated cryptographic modules within the scope of claims indicated above. SAIC offers no warranties or guarantees with respect to the above described compliance review. This letter does not imply an SAIC certification or product endorsement.

Please let us know if you have any questions.

Sincerely,

DM Sniegowski

Daun-Marie Sniegowski
Laboratory Director