SAIC
From Science to Solutions

Wednesday, September 1, 2010

To Whom It May Concern:

SAIC completed its conformance review of the Cisco System's **Web Security Appliance (WSA) S670 (Version: 6.5.0)** (the "Product") on Wednesday, August 25, 2010; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

1. Nitrox XL CN1510-NFBE FIPS Cryptographic Module (FIPS 140-2 Cert. #1360)

Specifically, SAIC's review confirmed that:

1. All cryptographic algorithms used for connections for accessing the Management GUI are offloaded to the validated Nitrox XL CN1510-NFBE FIPS Cryptographic Module.
2. All cryptographic algorithms used for SSH connections are offloaded to the validated Nitrox XL CN1510-NFBE FIPS Cryptographic Module.
3. All cryptographic algorithms used for by the HTTPs Proxy are offloaded to the validated Nitrox XL CN1510-NFBE FIPS Cryptographic Module.

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 claim`s 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,

Edward Morris
Laboratory Director

Science Applications International Corporation
6849 Old Dominion Drive, Suite 360 | McLean, VA 22101 | tel: 703.748.4551 | fax: 703.748.4552 | saic.com