CISCO

Cisco Systems, Inc.
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park
NC 27709
Phone: 919 392-2000
http://www.cisco.com

November 25, 2013

To Whom It May Concern

Cisco completed its conformance review of the Cisco Webex Meeting Server(CWMS) (software version: 1.5.1)("the Product") on November 15, 2013, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco Common Cryptographic Module (C3M) (FIPS 140-2 Cert. #1643)

2. RSA BSAFE Crypto-J JSAFE and JCE Software module (FIPS 140-2 Cert. #1503)

Specifically, Cisco'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 SSHv2, SIP-TLS and SRTP used for session establishment, are offloaded to Cisco Common Cryptographic Module (C3M) with FIPS 140-2 Cert. #1643.

3. All cryptographic algorithms used for Password Storage Encrypt/Decrypt operations, are offloaded to RSA BSAFE® Crypto-J JSAFE and JCE Software module with FIPS 140-2 Cert. #1503.

4. Bulk data encryption for the established SSHv2, SIP-TLS and SRTP secure connections use the Cisco Common Cryptographic Module (C3M) with FIPS 140-2 Cert. #1643.

5. Bulk data encryption for Password Storage Encrypt/Decrypt operation uses the RSA BSAFE® Crypto-J JSAFE and JCE Software Module with FIPS 140-2 Cert. #1503.

Details of Cisco's review, which consisted of source code review and operational testing, can be provided upon request.

Moreover, the FIPS conformance claims made for CWMS 1.1.1.107.A, verified by SAIC, hold true for CWMS 1.5.1 with no additions or removal of cryptographic services or cryptographic implementations.

The intention of this letter is to provide our assessment that the Product correctly integrates and uses validated cryptographic modules within the scope of the claims indicated above. Cisco offers no warranties or guarantees with respect to the above described conformance review. Furthermore, the Cryptographic Module Validation Program (CMVP) has not independently reviewed Cisco's analysis, testing or results.

Any questions regarding these statements may be directed to the Cisco Global Certification Team (certteam@cisco.com).

Thank you,

Ed Paradise
VP Engineering
Cisco TRIAD