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

October 16, 2014

To Whom It May Concern

Cisco completed its conformance review of Cisco WebEx Meetings Server (Version: 2.5)("the Product") on 3 September, 2014, and has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic modules:

1. Cisco FIPS Object Module (FIPS 140-2 Cert. #2100)
2. Cisco Common Cryptographic Module (C3M) (FIPS 140-2 Cert. #1643)
3. 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. Note: the cryptographic module supports pre-SP800-131 key strength (less than 112-bits). In order to operate in an approved mode of operation, applications must only use cryptographic services with key strength of 112-bit or greater.
2. All cryptographic algorithms used in SSH v2 and SIP-TLS for sessions establishment, are offloaded to Cisco FIPS Object Module with FIPS 140-2 Cert. #2100.
3. All cryptographic algorithms used in sRTP for session establishment, are offloaded to Cisco Common Cryptographic Module (C3M) with FIPS 140-2 Cert. #1643.
4. All cryptographic algorithms used for Password Storage Encrypt/Decrypt operation, are offloaded to RSA BSAFE® Crypto-J JSAFE and JCE Software Module with FIPS 140-2 Cert. #1503.
5. Bulk data encryption for the established SSH v2 and SIP-TLS secure connections use the Cisco FIPS Object Module with FIPS 140-2 Cert. #2100.
6. Bulk data encryption for the established sRTP secure connection use the Cisco Common Cryptographic Module (C3M) with FIPS 140-2 Cert. #1643.
7. 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 Cisco WebEx Meetings Server, version 2.0, verified by Leidos, hold true for Cisco WebEx Meetings Server, version 2.5, 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 Security and Trust Organization Engineering