



July 9, 2014

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

To Whom It May Concern:

Leidos completed its conformance review of the **Cisco Systems, Inc.'s Cisco WebEx Meetings Server v 2.0.1** (the "Product") on July 8, 2014; has found that the Product faithfully integrates the following FIPS 140-2 approved cryptographic module:

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, Leidos' 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 Leidos' review, which consisted of source code review and operational testing, are obtainable by special request.

Please note that for this review, Leidos only examined the Product features referenced above and while the Product may contain other features or functionality, LEIDOS 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 LEIDOS'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. LEIDOS offers no warranties or guarantees with respect to the above described compliance review. This letter does not imply an LEIDOS certification or product endorsement.

Sincerely,

A handwritten signature in blue ink, appearing to read 'W. Tung', is written over a light blue circular stamp.

William Tung  
Laboratory Manager