2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

June 19, 2019

Whom It May Concern:

Acumen Security verified that the following product faithfully embeds FIPS 140-2 validated cryptographic modules,

- Cisco Unified Communications Manager (CUCM) 12.5

During the review, Acumen Security confirmed that the following FIPS 140-2 cryptographic modules are incorporated into the product,

- Cisco FIPS Object Module (version 6.2), cert #2984
- Cisco Systems Kernel Crypto API Cryptographic Module, cert #3535
- Cisco Systems Libreswan Cryptographic Module, cert #3534
- Cisco Systems NSS Module, cert #3554

Acumen Security confirmed that the integrity for the incorporated **Cisco Systems Kernel Crypto API Cryptographic Module** is provided by the **Cisco Systems NSS Module**.

Acumen Security confirmed the **Cisco FIPS Object Module** provides cryptographic services through the following features: *Call processing, CA services, HTTPs, CTLs, SSH.*

Acumen Security confirmed the **Cisco Systems Kernel Crypto API provides cryptographic** services through the following feature: *IPsec Bulk Encryption.*

Acumen Security confirmed the **Cisco Systems Libreswan Cryptographic Module** provides cryptographic services through the following feature: *IKE/IPsec Key Derivation.*

Acumen Security confirmed the **Cisco FIPS Object Module** via **Cisco-J** provides cryptographic services through the following features: *LDAP over SSL, SOAP AXL, Disaster Recovery, Certificate Management.*

The above referenced modules provide all the cryptographic functionality for each of the services listed above, including:

- Session establishment supporting each service,
- All underlying cryptographic algorithms supporting each services' key derivation functions,
- Hashing for each service,
- Symmetric encryption for each service.

Additionally, Acumen Security confirmed that the above referenced cryptographic modules are initialized in a manner consistent with the instructions provided in their respective non-proprietary Security Policies.

Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties. This letter represents the independent opinions of Acumen Security and does not imply endorsement of the product by the CMVP or any other parties.

Sincerely,

Ashit Vora
Laboratory Director