September 20, 2019

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

To Whom It May Concern:

Gossamer Security Solutions, Inc. (hereinafter referred to as the "Gossamer") completed the FIPS testing on **Cisco Network Convergence System 1004 Cryptographic Module** with the firmware version **IOS XR 7.0** (the "Product") and submitted the conformance report (TID-28-9022-0000) to CMVP for validation on 9/20/2019. The submission is currently in CMVP coordination phase.

Specifically, Gossamer's tests confirmed that:

1. All cryptographic algorithms used for SSHv2 are provided from Cisco FIPS Object Module (v6.0) algorithm implementation.

2. All cryptographic algorithms used for TLS (v1.2) are provided from Cisco FIPS Object Module (v6.0) algorithm implementation.

3. All cryptographic algorithms used for SNMPv3 are provided from Cisco FIPS Object Module (v6.0) algorithm implementation.

4. All cryptographic algorithms used for OTNSec are provided from Cisco FIPS Object Module (v6.0) algorithm implementation.

It is important to note that the above services support some algorithms/key lengths that are no longer allowed by NIST Special Publication 800-131A. Please strictly follow up the steps in Security Policy, section Secure Operation to operate the module in the FIPS mode.

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

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. Gossamer offers no warranties or guarantees with respect to the above described compliance review. This letter does not imply a Gossamer certification or product endorsement.

Please let us know if you have any questions.

Sincerely,

Edward D. Morris
Laboratory Director