![CGI logo]

July 25th, 2016

To whom it may concern,

CGI Information Systems and Management Consultants Inc. (CGI) verified that the following software faithfully embeds a FIPS 140 cryptographic module,

- IOS XE 3.16

The referenced software is known to operate on the following routing platforms,

- CSR 1000V

As part of the review, the software was tested on the following products,

- CSR1000V on Cisco UCS E120E
- CSR1000V on Cisco UCS E120S

During the course of the vendor provided documentation review, operational testing of the referenced software running on the listed platforms and source code review, CGI confirmed that the following Cryptographic module is properly incorporated into the product:

- IOS Common Crypto Module (IC2M), Rel 5 and FIPS 140-2 certificate #2388

CGI confirmed that the following features leverage the embedded module to provide cryptographic services:
- SSH,
- SNMP,
- SSL/TLS
- IPsec

Additionally, CGI confirmed that the above referenced embedded cryptographic module is initialized in a manner consistent with the instructions provided in the non-proprietary Security Policy. Details of the verification may be obtained from Cisco Systems, Inc. at the request of interested parties.

This letter represents the independent opinions of CGI and does not imply endorsement of the product by the CMVP or any other parties.

Regards,

Marc Boire
Laboratory Director, CGI IT Security Evaluation and Test Facility