



February 27, 2026

To Whom It May Concern:

A compliance review of IOS XR version 25.4 ("the Product") deployed in the following platforms:

- Cisco Network Convergence System (NCS) 1004 Router
- Cisco Network Convergence System (NCS) 1010 Router
- Cisco Network Convergence System (NCS) 1014 Router

was completed and found that the Product incorporates the following FIPS 140-3 validated cryptographic module:

- CiscoSSL FIPS Provider version 8.0 (Certificate [#5430](#))

Cisco confirms that the cryptographic module listed above provides cryptographic services for the following as applicable:

- SSHv2
- SNMPv3
- TLSv1.2/TLSv1.3

The review/testing confirmed that:

1. The cryptographic module (mentioned above) does initialize in a manner that is compliant with its Security Policy.
2. All applicable cryptographic algorithms used for the services listed above are handled within the cryptographic module.
3. All applicable underlying cryptographic algorithms support each service's key derivation function.

This letter has been generated in accordance with guidance provided by the Cryptographic Module Validation Program ([CMVP](#)). The CMVP has not independently evaluated this compliance review.

Any questions regarding these statements may be directed via e-mail to the Cisco Global Certification Team (GCT) at [certteam@cisco.com](mailto:certteam@cisco.com).

Sincerely,

A handwritten signature in black ink that reads "Edward D. Paradise".

Ed Paradise  
Cisco Senior Vice President  
Foundational & Government Security