Sept 2, 2025

To Whom It May Concern:

A compliance review of Cisco Provider Connectivity Assurance Sensor Management version 25.07 (“the Product”) deployed in the following platforms:

Various network elements

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

- BC-FJA (Bouncy Castle FIPS Java API) (Certificate #4943)

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

- SSHv2.0, TLSv1.2 and 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.

Sincerely,

Edward D Paradise

Ed Paradise
Cisco Senior Vice President
Foundational & Government Security