September 22, 2025

To Whom It May Concern,

A compliance review of Cisco Identity Services Module release 3.5 ("the Product") deployed in the following platforms:

- SNS-3715
- SNS-3755
- SNS-3795
- SNS-3815
- SNS-3855
- SNS-3895
- ISE Virtual Deployment

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

- Cisco FIPS Object Module (FOM) 7.3a (Certificate #4747)
- Cisco Linux Kernel FIPS Object Module (KFOM) 1.0 (Certificate #4744)
- Bouncy Castle Java API 2.0 (Certificate #4743)

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

- EAP-TLS (FOM 7.3a)
- EAP-FAST (FOM 7.3a)
- LDAPS (FOM 7.3a)
- IPSec (Control Plane FOM 7.3a and Data Plane KFOM 1.0)
- SSHv2 (FOM 7.3a)
- TCNAC – Tenable (Bouncy Castle 2.0)
- PxGrid (Bouncy Castle 2.0)
- PxGrid Cloud (FOM 7.3a)

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