



January 14, 2026

To Whom It May Concern,

A compliance review of Cisco Cyber Vision, version 5.3 ("the Product") deployed in the following platforms:

*Cisco Catalyst IE3300 Rugged Series switch*  
*Cisco Catalyst IE3400 Rugged Series switch*  
*Cisco Catalyst IE3400 Heavy Duty Series switch*  
*Cisco Catalyst IR1100 Rugged Series Routers*  
*Cisco Catalyst IR8300 Rugged Series Router*

*Cisco Catalyst 9300 Series switch*  
*Cisco Catalyst 9400 Series switch*  
*Cisco Catalyst IR1800 Rugged Series Routers*  
*Cisco Catalyst IE9300 Rugged Series Switches*  
*Cyber Vision Sensor Docker application (deployed on FIPS-validated Docker stack)*

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

- Cisco FIPS Object Module version 7.3a (Certificate [#4747](#))

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

- TLSv1.2, TLSv1.3 and SSHv2 – FOM version 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](mailto:certteam@cisco.com).

Sincerely,

Ed Paradise  
Cisco Senior Vice President  
Foundational & Government Security