REPORT OF THE INDEPENDENT ACCOUNTANT

To the management of Cisco Systems, Inc. ("Cisco")

We have examined Cisco management's assertion that for its Certification Authority (CA) operations at Research Triangle Park, North Carolina, USA, throughout the period October 1, 2018 to September 30, 2019 for its CAs as enumerated in Attachment A, for SSL Baseline Requirements and Network Security Requirements, Cisco has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - Cisco SSL Issuance Subordinated CA, XSSL-R2, Version 2.8 Certification Practice Statement

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Baseline Requirements v1.6.6, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by Cisco)

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

Based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3. Cisco's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion, based on our examination.

The relative effectiveness and significance of specific controls at Cisco and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. Our examination did not extend to controls at individual subscriber and relying party locations and we have not evaluated the effectiveness of such controls.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of the nature and inherent limitations of controls, Cisco's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

In our opinion management's assertion, as referred to above, is fairly stated, in all material respects.

This report does not include any representation as to the quality of Cisco's services other than its CA operations at Research Triangle Park, North Carolina, USA, nor the suitability of any of Cisco's services for any customer's intended purpose.

Cisco's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Sensiba San Filippo LLP
Certified Public Accountants
San Jose, CA
November XX, 2019

CISCO SYSTEMS MANAGEMENT'S ASSERTION

Cisco Systems, Inc. ("Cisco") operates the Certification Authority (CA) services known as Cisco SSL Issuance Subordinated CA, XSSL-R2, and provides SSL CA services.

Cisco management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at Research Triangle Park, North Carolina, USA, throughout the period October 1, 2018 to September 30, 2019, Cisco has:

- disclosed its SSL certificate lifecycle management business practices in its:
    - Cisco SSL Issuance Subordinated CA, XSSL-R2, Version 2.8 Certification Practice Statement

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Baseline Requirements v1.6.6, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by Cisco)

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3.

<Signoff Name and Title>
<Date that matches the audit opinion date>

Attachment A:

The list of keys and certificates covered by this assessment are as follows:

Key Name (Role)	Cisco XSSL-R2 (Issuing CA)		
Certificate Issuer	C = US, O = Cisco Systems, CN = Cisco RXC-R2		
Certificate Subject	C = US, O = Cisco Systems, CN = Cisco XSSL-R2		
Key Size	RSA-2048	Signing Algorithm	SHA-256
SHA-1 Fingerprint			
AC:23:0A:22:B9:FE:19:FC:5F:A0:FD:D0:8D:91:54:F9:8F:7F:B6:AE			
SHA-256 Fingerprint			
CB:28:62:ED:0C:9D:07:EB:68:93:84:D8:12:B8:96:D2:05:F0:AE:2A:A5:5C:F4:AC:0D:67:CF:24:BA:06:9E:EE			