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, Cisco has

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - Cisco Root CA RXC-R2, Version 2.6 Certification Practice Statement;
    - Cisco Root CA RXC-R2, Version 1.8 Certificate Policy; and
    - Cisco SSL Issuance Subordinated CA, XSSL-R2, Version 2.8 Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
    - Cisco's Certification Practice Statements are consistent with its Certificate Policies
    - Cisco provides its services in accordance with its Certificate Policies and Certification Practice Statements
- maintained effective controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by Cisco); and
    - subordinate CA certificate requests are accurate, authenticated, and approved
- 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

Based on the WebTrust Principles and Criteria for Certification Authorities v2.1. 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.

Cisco does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our examination did not extend to controls that would address those criteria.

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 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 Root CA RXC-R2 and Cisco SSL Issuance Subordinated CA XSSL-R2, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation and management

The management of Cisco is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website, CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to Cisco's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

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

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its:
    - Cisco Root CA RXC-R2, Version 2.6 Certification Practice Statement;
    - Cisco Root CA RXC-R2, Version 1.8 Certificate Policy; and
    - Cisco SSL Issuance Subordinated CA, XSSL-R2, Version 2.8 Certification Practice Statement
- maintained effective controls to provide reasonable assurance that:
    - Cisco's Certification Practice Statements are consistent with its Certificate Policies
    - Cisco provides its services in accordance with its Certificate Policies and Certification Practice Statements

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

- 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

based on the WebTrust Principles and Criteria for Certification Authorities v2.1, including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security

Physical & Environmental Security

- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

<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 RXC-R2 (Root Key)		
Certificate Issuer	[Self]		
Certificate Subject	C = US, O = Cisco Systems, CN = Cisco RXC-R2		
Key Size	RSA-2048	Signing Algorithm	SHA-256
SHA-1 Fingerprint			
2C:8A:FF:CE:96:64:30:BA:04:C0:4F:81:DD:4B:49:C7:1B:5B:81:A0			
SHA-256 Fingerprint			
22:9C:CC:19:6D:32:C9:84:21:CC:11:9E:78:48:6E:EB:EF:60:3A:EC:D5:25:C6:B8:8B:47:AB:B7:40:69:2B:96			

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			