REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

To the Management of Internet Security Research Group (ISRG):

Scope

We have examined ISRG management's assertion that for its Certification Authority (CA) operations at its Salt Lake City, Utah, and Centennial, Colorado, locations, for the program known as Let's Encrypt throughout the period September 1, 2018, to August 31, 2019, for its root and subordinate CA certificates as listed in Appendix A, ISRG has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement (v2.6); and
  - Certificate Policy (v2.3)

  including its commitment to provide SSL Certificates in conformity with the CA/Browser Forum Requirements on the ISRG website, 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 ISRG)
- 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 – Version 2.3 (herein referred to as the "WebTrust for CAs - SSL Baseline Criteria").

Internet Security Research Group's Responsibilities

ISRG'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 ISRG 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.

Independent Certified Public Accountant's Responsibilities

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.

Inherent Limitations

Because of the nature and inherent limitations of controls, ISRG'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.

Opinion

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

Emphasis on Matters

ISRG has disclosed the following matters during the review period:

- ISRG publicly disclosed an incident on August 26, 2019 in which incorrect OCSP responses were served under certain rare conditions. A fix was developed and deployed without delay and it was determined that the issue described did not impact ISRG's ability to meet the WebTrust for CAs - SSL Baseline Criteria.
- ISRG publicly disclosed an incident on August 29, 2019 in which incorrect OCSP responses were served for a small number of precertificates. A fix was developed and deployed without delay and it was determined that the issue described did not impact ISRG's ability to meet the WebTrust for CAs - SSL Baseline Criteria.
- ISRG internally identified a software misconfiguration documented on June 29, 2019, and the software correction implemented on July 29, 2019. In relation to Criterion 8.4 in Principle 2 of the WebTrust for CAs - SSL Baseline Criteria which states "The CA maintains controls to provide reasonable assurance that it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken", ISRG identified an issue with the automated certificate content checking tool used for ongoing self-assessments to verify compliance with the CA/Browser Forum Baseline Requirements (hereafter referred to as Baseline Requirements) and ISRG's Certificate Policy and Certification Practice Statement in which a minimum of 3% of issued certificates are examined on at least a quarterly basis. The software misconfiguration resulted in some certificates not being properly scanned for validation. Upon identifying the issue, ISRG implemented a software change to correct the misconfiguration. ISRG ran the updated certificate content checking tool against each certificate issued from the beginning of the review period to the date of the software correction and through the end of the review period to confirm that each certificate was issued in compliance with the Baseline Requirements at the time of issuance.

During our assessment, Schellman performed testing of certificate issuance, on a sample basis, and noted that there were no certificate deficiencies identified in any of the samples tested. As a result, our opinion is not modified with respect to these matters.

This report does not include any representation as to the quality of ISRG's services other than its CA operations at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, nor the suitability of any of ISRG's services for any customer's intended purpose.

ISRG's use of the WebTrust Principles and Criteria 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.

SCHELLMAN & COMPANY, LLC

Schellman & Company, LLC
Certified Public Accountants
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
November 11, 2019

ASSERTION OF MANAGEMENT AS TO ITS DISCLOSURE OF ITS PRACTICES AND ITS CONTROLS OVER ITS SSL CERTIFICATION AUTHORITY OPERATIONS DURING THE PERIOD SEPTEMBER 1, 2018, TO AUGUST 31, 2019

Internet Security Research Group (ISRG) operates the Certification Authority (CA) services known as Let's Encrypt for its root and subordinate CA certificates as listed in Appendix A and provides SSL CA services.

ISRG management has assessed its controls over its Let's Encrypt SSL CA services. Based on that assessment, in providing its SSL Certification Authority (CA) services at its Salt Lake City, Utah, and Centennial, Colorado, locations throughout the period September 1, 2018, to August 31, 2019, ISRG has:

- Disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement (v2.6); and
  - Certificate Policy (v2.3)

  including its commitment to provide SSL Certificates in conformity with the CA/Browser Forum Requirements on the ISRG website, 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 ISRG)
- 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 – Version 2.3.

During the course of the assessment, ISRG disclosed the following matters during the review period:

- ISRG publicly disclosed an incident on August 26, 2019 in which incorrect OCSP responses were served under certain rare conditions. A fix was developed and deployed without delay and it was determined that the issue described did not impact ISRG's ability to meet the WebTrust for CAs - SSL Baseline Criteria.
- ISRG publicly disclosed an incident on August 29, 2019 in which incorrect OCSP responses were served for a small number of precertificates. A fix was developed and deployed without delay and it was determined that the issue described did not impact ISRG's ability to meet the WebTrust for CAs - SSL Baseline Criteria.
- ISRG internally identified a software misconfiguration documented on June 29, 2019, and the software correction implemented on July 29, 2019. In relation to Criterion 8.4 in Principle 2 of the WebTrust for CAs - SSL Baseline Criteria which states "The CA maintains controls to provide reasonable assurance that it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) of the Certificates issued during the period commencing

immediately after the previous self-assessment samples was taken", ISRG identified an issue with the automated certificate content checking tool used for ongoing self-assessments to verify compliance with the CA/Browser Forum Baseline Requirements (hereafter referred to as Baseline Requirements) and ISRG's Certificate Policy and Certification Practice Statement in which a minimum of 3% of issued certificates are examined on at least a quarterly basis. The software misconfiguration resulted in some certificates not being properly scanned for validation. Upon identifying the issue, ISRG implemented a software change to correct the misconfiguration. ISRG ran the updated certificate content checking tool against each certificate issued from the beginning of the review period to the date of the software correction and through the end of the review period to confirm that each certificate was issued in compliance with the Baseline Requirements at the time of issuance.

Joshua Aas
Executive Director
Internet Security Research Group
November 11, 2019

APPENDIX A – ISRG ROOT AND ISSUING CAs

Distinguished Name	Certificate SHA-256 Fingerprint
Subject: C=US, O=Internet Security Research Group, CN=ISRG Root X1	96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1	BDEE0D7C8F9C278F14EA9B6A4F90ED665A9F56DB0A56B1CDDA6765912F398A5E
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2	E4EB54A7FFA552EF64D8E1AE338B69BE909C29E6AF57170A2F6F44DF225E5A14
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	731D3D9CFAA061487A1D71445A42F67DF0AFCA2A6C2D2F98FF7B3CE112B1F568
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4	5DE9152BED31FA0515DD1FC746133F1327562EF72A84CF2D2403E748A604D0D4
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X1	7FDCE3BF4103C2684B3ADBB5792884BD45C75094C217788863950346F79C90A3
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X2	EC0C6CA496A67A13342FEC5221F68D4B3E53B1BC22F6E4BCCC9C68F0415CDEA4
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3	25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D
Subject: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X4	A74B0C32B65B95FE2C4F8F098947A68B695033BED0B51DD8B984ECAE89571BB6