REPORT OF THE INDEPENDENT ACCOUNTANT

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

Scope

We have examined ISRG’s assertion that for its Certification Authority (CA) operations at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA locations, for the program known as Let’s Encrypt, for its CAs as enumerated in Appendix A, ISRG has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - Certification Practice Statement (v4.1, v4.2, v4.3); and
  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 throughout the period September 1, 2021, to August 31, 2022, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5.

ISRG does not manage any subscriber private keys, does not receive any subordinate CA requests from outside entities, and does not issue any subordinate CAs for outside entities. Accordingly, our examination did not extend to controls that would address those criteria.

Certification Authority’s Responsibilities

ISRG’s management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5.

Practitioner’s Responsibilities

Our responsibility is to express an opinion on ISRG’s management’s assertion based on our examination. 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.
We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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.

Inherent Limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion
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 ISRG’s services other than its SSL 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.

Emphasis of Matters
ISRG has disclosed that during the period September 1, 2021, to August 31, 2022, the following incidents were identified and disclosed to the CA/B Forum community as follows:

- Mozilla Bug ID 1729567: On September 5, 2021, ISRG was made aware via their internal monitoring systems that the system responsible for updating OCSP responses (ocsp-updater) had fallen two (2) hours behind the target 3-day update schedule. A warning alert was fired, but not received by the on-call personnel due to being configured as a working-hours-only alert. ISRG signs and publishes OCSP responses with a validity interval of 7 days. Automated systems are configured to produce updates for all OCSP responses whose Update field is three (3) or more days in the past. ISRG fixed the proximate cause by updating their production configuration files to now use the correct “serialSuffixShards” key and their ocsp-updater instances are not performing duplicate work.

- Mozilla Bug ID 1735247: On October 11, 2021, ISRG was notified via their cert-prob-reports e-mail that their software was potentially violating SC48v2 and ISRG had misissued certificates. On October 1, 2021, a new Baseline Requirements revision (Ballot SC48v2) went into effect stating that “the Fully-Qualified Domain Name or the FQDN portion of the Wildcard Domain Name MUST consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels”. ISRG had reviewed the requirement before the effective date but missed a case to forbid a Reserved LDH Label when a hyphen is its second character. The code incorrectly allowed domains like a---foo.example.com but correctly forbade names like ab--foo.example.com. ISRG verified the claim and stopped CA issuance while a fix was deployed. An audit of certificates issued since October 1, 2021, revealed 7 affected certificates. The certificates were revoked within 24 hours of the report.

- Mozilla Bug ID 1751984 and 1753123: On January 25, 2022, ISRG was notified of an instance of non-compliance in their implementation of the TLS-ALPN-01 challenge type (RFC 8737), which is the basis of the TLS Using ALPN validation method (BRs Section 3.2.2.4.20). ISRG’s TLS-ALPN-01 client code was not setting a specific minimum TLS version, and was therefore using Go’s default minimum TLS version, which is TLS 1.0. While it is likely that many if not most validations were performed over TLS 1.2 or higher, ISRG does not log the negotiated TLS version as part of the validation data, so it must be assumed that all validations conducted using this method could have been affected. Both issues were fixed and all unexpired certificates which contained identifiers validated using the TLS-ALPN-01 challenge type prior to the fix were revoked by January 30, 2022, five days from when ISRG was made aware that they were not issued in accordance with the Baseline Requirements. In addition, as part of the remediation process for Bug 1751984, ISRG discovered a small number of entries in their database for which pre-certificate data was stored but did not have corresponding certificate status (particularly, OCSP response) data stored. These certificates never had OCSP data available. As no authoritative records for these certificates were
available, all requests for their OCSP responses resulted in an “unauthorized” response, as required by RFC 5019, Section 2.2.3 and RFC 6960, Section 2.3. ISRG populated OCSP responses for all affected certificates and fixed the error which allowed certificates without corresponding OCSP responses to be stored in their database.

- Mozilla Bug ID 1752670: On January 28, 2022, ISRG was notified that their TLS ALPN validation implementation did not match the specification. In particular, RFC 8737 states that “The ACME server verifies that...he certificate returned contains a subjectAltName extension containing the dNSName being validated and no other entries.” The Let's Encrypt implementation validated that only one dNSName was present, but did not ensure that there were no entries of other types, such as IP addresses. The issue was resolved and affected certificates were revoked by February 2, 2022.

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.

Use of the WebTrust Seal

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
Certified Public Accountants
4010 W Boy Scout Blvd, Suite 600
Tampa, Florida 33607
November 08, 2022
ISRG MANAGEMENT’S ASSERTION

Internet Security Research Group (ISRG) operates the Certification Authority (CA) services known as Let’s Encrypt and provides SSL CA services.

ISRG management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, except for the matters described in the emphasis-of-matters paragraphs below, in providing its SSL CA services at its Salt Lake City, Utah, USA, and Centennial, Colorado, USA, locations, for its root and subordinate CA certificates enumerated in Appendix A, ISRG has:

- disclosed its SSL certificate lifecycle management business practices in its certification practice statement and certificate policy as follows:
  - Certification Practice Statement (v4.1, v4.2, v4.3); and

  including its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Requirements on the ISRG website, and provided such services in accordance with its disclosed business 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 throughout the period of September 1, 2021, to August 31, 2022, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.5.

Emphasis of Matters

ISRG has disclosed that during the period September 1, 2021, to August 31, 2022, the following incidents were identified and disclosed to the CA/B Forum community as follows:

- Mozilla Bug ID 1729567: On September 5, 2021, ISRG was made aware via their internal monitoring systems that the system responsible for updating OCSP responses (ocsp-updater) had fallen two (2) hours behind the target 3-day update schedule. A warning alert was fired, but not received by the on-call personnel due to being configured as a working-hours-only alert. ISRG signs and publishes OCSP responses with a validity interval of 7 days. Automated systems are configured to produce updates for all OCSP responses whose this Update field is three (3) or more days in the past. ISRG fixed the proximate cause by updating their production configuration files to now use the correct "serialSuffixShards" key and their ocsp-updater instances are not performing duplicate work.

- Mozilla Bug ID 1735247: On October 11, 2021, ISRG was notified via their cert-prob-reports e-mail that their software was potentially violating SC48v2 and ISRG had misissued certificates. On October 1, 2021, a new Baseline Requirements revision (Ballot SC48v2) went into effect stating that “the Fully-Qualified
Domain Name or the FQDN portion of the Wildcard Domain Name MUST consist solely of Domain Labels that are P-Labels or Non-Reserved LDH Labels”. ISRG had reviewed the requirement before the effective date but missed a case to forbid a Reserved LDH Label when a hyphen is its second character. The code incorrectly allowed domains like a---foo.example.com but correctly forbade names like ab--foo.example.com. ISRG verified the claim and stopped CA issuance while a fix was deployed. An audit of certificates issued since October 1, 2021, revealed 7 affected certificates. The certificates were revoked within 24 hours of the report.

- Mozilla Bug ID 1751984 and 1753123: On January 25, 2022, ISRG was notified of an instance of non-compliance in their implementation of the TLS-ALPN-01 challenge type (RFC 8737), which is the basis of the TLS Using ALPN validation method (BRs Section 3.2.2.4.20). ISRG’s TLS-ALPN-01 client code was not setting a specific minimum TLS version, and was therefore using Go’s default minimum TLS version, which is TLS 1.0. While it is likely that many if not most validations were performed over TLS 1.2 or higher, ISRG does not log the negotiated TLS version as part of the validation data, so it must be assumed that all validations conducted using this method could have been affected. Both issues were fixed and all unexpired certificates which contained identifiers validated using the TLS-ALPN-01 challenge type prior to the fix were revoked by January 30, 2022, five days from when ISRG was made aware that they were not issued in accordance with the Baseline Requirements. In addition, as part of the remediation process for Bug 1751984, ISRG discovered a small number of entries in their database for which pre-certificate data was stored but did not have corresponding certificate status (particularly, OCSP response) data stored. These certificates never had OCSP data available. As no authoritative records for these certificates were available, all requests for their OCSP responses resulted in an “unauthorized” response, as required by RFC 5019, Section 2.2.3 and RFC 6960, Section 2.3. ISRG populated OCSP responses for all affected certificates and fixed the error which allowed certificates without corresponding OCSP responses to be stored in their database.

- Mozilla Bug ID 1752670: On January 28, 2022, ISRG was notified that their TLS ALPN validation implementation did not match the specification. In particular, RFC 8737 states that “The ACME server verifies that…the certificate returned contains…a subjectAltName extension containing the dNSName being validated and no other entries.” The Let's Encrypt implementation validated that only one dNSName was present, but did not ensure that there were no entries of other types, such as IP addresses. The issue was resolved and affected certificates were revoked by February 2, 2022.

Joshua Aas
Executive Director
Internet Security Research Group
November 08, 2022
## APPENDIX A – ISRG ROOT AND ISSUING CAs

<table>
<thead>
<tr>
<th>Distinguished Name</th>
<th>Certificate SHA-256 Fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1</td>
<td>96BCEC06264976F37460779ACF28C5A7CFE8A3C0AAE11A8FFCEE05C0BDDF08C6</td>
</tr>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X2</td>
<td>69729B8E15A86EFC177A57AFB7171DFC64ADD28C2FCA8CF1507E34453CCB1470</td>
</tr>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X2</td>
<td>8B05B68CC6599E5ED0FCB38F2C942FBFD200E6F2FF9F85D63C6994EF5E0B02701</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3</td>
<td>731D3D9CFAAA061487A1D71445A42F67DF0AFCA2A6C2D2F98FF7B3C112B1F568</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X4</td>
<td>5DE9152BED31FA0515DD1FC746133F1327562EF72A84CF2D2403E74A604D0D4</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = R3</td>
<td>67ADD1166B20AE61B8F5FC96813C04C2AA589960796865572A3C7E737613DFD</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = R4</td>
<td>1A07529A8B3F01D231DFAD2ABDF71899200BB65CD7E03C59FA82272533355B74</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = E1</td>
<td>46494E30379059DF18BE52124305E606FC59070E5B21076CE113954B60517CDA</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = E2</td>
<td>BACDE0463053CE1D62F8BE74370BBAE79D4FCAF19FC07643AEF195E6A59BD578</td>
</tr>
</tbody>
</table>

The following certificates were signed by IdenTrust for ISRG.

<table>
<thead>
<tr>
<th>Distinguished Name</th>
<th>Certificate SHA-256 Fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1</td>
<td>6D99FB265EB1C5B3744765FCBC648F3CD8E1BFFAFDC4C2F99B9D47CF7FF1C24F</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X1</td>
<td>7FDCE3BF4103C2684B3A4BB5792884BD45C75094C21778863950346F79C90A3</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X1</td>
<td>23D29B9707396BCCA317F9EF1B1E6A626C4E481283CD85F74A516FF6CAB997ED</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X2</td>
<td>EC0C6CA496A67A13342FEC5221F68D4B3E53B1BC22F6E4BCC9C68F0415CDEA4</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X2</td>
<td>2F45659D64DC74CCEC9E2A4290715828F95FA8CC7A6C8800D3968F14DFCF1DB7</td>
</tr>
<tr>
<td>Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3</td>
<td>25847D668EB4F04FDD40B12B6B0740C567DA7D024308EB6C2C96FE41D9DE218D</td>
</tr>
</tbody>
</table>
## APPENDIX B– OTHER INCIDENTS DISCLOSED BY ISRG

The following incident(s) occurred prior to the audit period and disclosed because the associated Mozilla Bugzilla ticket was open at some point during the audit period.

<table>
<thead>
<tr>
<th>Mozilla Bugzilla ID</th>
<th>Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1715672</td>
<td>2021.06.09</td>
<td>Let's Encrypt: Failure to revoke for Certificate Lifetime Incident</td>
</tr>
<tr>
<td>1715455</td>
<td>2021.06.09</td>
<td>Let's Encrypt: certificate lifetimes 90 days plus one second</td>
</tr>
</tbody>
</table>