BDO

Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 S Hanley Rd, #800
St. Louis, MO 63105

REPORT OF THE INDEPENDENT ACCOUNTANT

To the Management of Microsoft Corporation Core Services Engineering & Operations ("Microsoft CSEO"):

We have examined for Microsoft CSEO's certification authority ("CA") operations at Redmond, Washington,

- Microsoft CSEO's disclosure of its SSL certificate lifecycle management business practices in its:
  - DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs, Version 2.0, Effective May 1, 2018; and
  - Microsoft IT PKI Certificate Policy/Certification Practice Statement for SSL CAs, Version 1.5, Effective October 30, 2017

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft CSEO repository

- the provision of such services in accordance with its disclosed practices

- the effectiveness of its controls over:
  - key and SSL certificate integrity;
  - the authenticity and confidentiality of SSL subscriber and relying party information;
  - continuity of key and SSL certificate lifecycle management operations;
  - development, maintenance, and operation of CA systems integrity; and
  - meeting the network and certificate system security requirements set forth by the CA/Browser Forum

throughout the period February 1, 2018 to June 30, 2018 for its CAs enumerated in Attachment A, in scope for SSL Baseline Requirements and Network Security Requirements.

Microsoft CSEO's management is responsible for these disclosures and for maintaining effective controls based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3. Our responsibility is to express an opinion based on our examination.

The relative effectiveness and significance of specific controls at Microsoft CSEO 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, throughout the period February 1, 2018 to June 30, 2018, for its CAs enumerated in Attachment A, in all material respects, Microsoft CSEO:

- disclosed its SSL certificate lifecycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft CSEO repository

- provided such services in accordance with its disclosed practices

- maintained effective controls over:
  - key and SSL certificate integrity;
  - the authenticity and confidentiality of SSL subscriber and relying party information;
  - continuity of key and SSL certificate lifecycle management operations;
  - development, maintenance, and operation of CA systems integrity; and
  - meeting 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.

Because of the nature and inherent limitations of controls, Microsoft CSEO'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.

During our examination, we noted the following which caused a qualification of our opinion:

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		Control Deficiency Noted
2-7.3	The CA maintains controls to provide reasonable assurance that audit logs generated are retained for at least seven years.	Firewall and router logs are only being retained for two years.

In our opinion, except for the effect of the matter described in the preceding table, throughout the period February 1, 2018 to June 30, 2018, Microsoft CSEO has, in all material respects:

- disclosed its SSL certificate lifecycle management business practices in its:
  - DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs, Version 2.0, Effective May 1, 2018, and
  - Microsoft IT PKI Certificate Policy/Certification Practice Statement for SSL CAs, Version 1.5, Effective October 30, 2017

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft CSEO repository

- provided such services in accordance with its disclosed practices

- maintained effective controls over:

- key and SSL certificate integrity;
- the authenticity and confidentiality of SSL subscriber and relying party information;
- continuity of key and SSL certificate lifecycle management operations;
- development, maintenance, and operation of CA systems integrity; and
- meeting 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.

This report does not include any representation as to the quality of Microsoft CSEO's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.3, nor the suitability of any of Microsoft CSEO's services for any customer's intended purpose.

BDO USA, LLP

St. Louis, Missouri
September 17, 2018

ATTACHMENT A - IN-SCOPE CAs

CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint

CN = Microsoft IT SSL SHA1
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	07 27 aa 46	7b 65 52 4c 60 06 ce 5f d2 93 c3 05 10 43 c6 d1 38 4d 62 6a	9d 56 01 ca ca f8 97 1b f0 54 fa 23 3f e6 04 df 17 bb 45 8d b2 06 f1 0c a0 be bc a4 c5 46 6b ce

CN = Microsoft IT SSL SHA2
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	07 27 aa 47	97 ef f3 02 86 77 89 4b dd 4f 9a c5 3f 78 9b ee 5d f4 ad 86	23 99 98 3e 99 70 3e bd 01 ce a4 66 c1 07 99 81 0c 4b a6 2a 8d 61 b8 81 70 a3 34 dc d6 1b b2 0f

CN = Microsoft IT TLS CA 1
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	08 b8 7a 50 1b be 9c da 2d 16 4d 3e 39 51 bf 55	41 7e 22 50 37 fb fa a4 f9 57 61 d5 ae 72 9e 1a ea 7e 3a 42	4f f4 04 f0 2e 2c d0 01 88 f1 5d 1c 00 f4 b6 d1 e3 8b 5a 39 5c f8 53 14 ea eb a8 55 b6 a6 4b 75

CN = Microsoft IT TLS CA 2
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	0f 2c 10 c9 5b 06 c0 93 7f b8 d4 49 f8 3e 85 69	54 d9 d2 02 39 08 0c 32 31 6e d9 ff 98 0a 48 98 8f 4a df 2d	4e 10 7c 98 1b 42 ac be 41 c0 10 67 e1 6d 44 db 64 81 4d 41 93 e5 72 31 7e a0 4b 87 c7 9c 47 5f

CN = Microsoft IT TLS CA 4
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	0b 6a b3 b0 3e b1 a9 f6 c4 60 92 6a a8 cd fe b3	8a 38 75 5d 09 96 82 3f e8 fa 31 16 a2 77 ce 44 6e ac 4e 99	5f fa c4 3e 0d dc 5b 4a f2 b6 96 f6 bc 4d b7 e9 1d f3 14 bb 8f e0 d0 71 3a 0b 1a 7a d2 a6 8f ac

CN = Microsoft IT TLS CA 5
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	08 88 cd 52 5f 19 24 44 4d 14 a5 82 91 de b9 52	ad 89 8a c7 3d f3 33 eb 60 ac 1f 5f c6 c4 b2 21 9d db 79 b7	f0 ee 59 14 ed 94 c7 25 2d 05 8b 4e 39 80 8a ee 6f a8 f6 2c f0 97 4f b7 d6 d2 a9 df 16 e3 a8 7f

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 706 7329
www.microsoft.com

Microsoft

Microsoft Corporation Core Services Engineering & Operations Management's Assertion

Microsoft Corporation Core Services Engineering & Operations ("Microsoft CSEO") operates the Certification Authority ("CA") services for its CAs enumerated in Attachment A in scope for SSL Baseline and Network Security Requirements and provides SSL CA services.

Microsoft CSEO's management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL CA services at Redmond, Washington, throughout the period February 1, 2018 to June 30, 2018, Microsoft CSEO has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - DSRE PKI Certificate Policy/Certification Practice Statement for TLS CAs, Version 2.0, Effective May 1, 2018; and
  - Microsoft IT PKI Certificate Policy/Certification Practice Statement for SSL CAs, Version 1.5, Effective October 30, 2017

  including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the Microsoft CSEO repository, 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

- 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, except for the effect of the matter noted below:

Impacted WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security		Control Deficiency Noted
2.7.3	The CA maintains controls to provide reasonable assurance that audit logs generated are retained for at least seven years.	Firewall and router logs are only being retained for two years. **Management Response** New policies have been implemented to ensure new firewall logs will be stored for at least 7 years.

Biju Mathew
Principal Service Engineer Manager, Identity Access Management
September 17, 2018

ATTACHMENT A - IN-SCOPE CAs

CA	Serial Number	SHA1 Thumbprint	SHA2 Thumbprint

CN = Microsoft IT SSL SHA1
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	07 27 aa 46	7b 65 52 4c 60 06 ce 5f d2 93 c3 05 10 43 c6 d1 38 4d 62 6a	9d 56 01 ca ca f8 97 1b f0 54 fa 23 3f e6 04 df 17 bb 45 8d b2 06 f1 0c a0 be bc a4 c5 46 6b ce

CN = Microsoft IT SSL SHA2
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	07 27 aa 47	97 ef f3 02 86 77 89 4b dd 4f 9a c5 3f 78 9b ee 5d f4 ad 86	23 99 98 3e 99 70 3e bd 01 ce a4 66 c1 07 99 81 0c 4b a6 2a 8d 61 b8 81 70 a3 34 dc d6 1b b2 0f

CN = Microsoft IT TLS CA 1
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	08 b8 7a 50 1b be 9c da 2d 16 4d 3e 39 51 bf 55	41 7e 22 50 37 fb fa a4 f9 57 61 d5 ae 72 9e 1a ea 7e 3a 42	4f f4 04 f0 2e 2c d0 01 88 f1 5d 1c 00 f4 b6 d1 e3 8b 5a 39 5c f8 53 14 ea eb a8 55 b6 a6 4b 75

CN = Microsoft IT TLS CA 2
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	0f 2c 10 c9 5b 06 c0 93 7f b8 d4 49 f8 3e 85 69	54 d9 d2 02 39 08 0c 32 31 6e d9 ff 98 0a 48 98 8f 4a df 2d	4e 10 7c 98 1b 42 ac be 41 c0 10 67 e1 6d 44 db 64 81 4d 41 93 e5 72 31 7e a0 4b 87 c7 9c 47 5f

CN = Microsoft IT TLS CA 4
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	0b 6a b3 b0 3e b1 a9 f6 c4 60 92 6a a8 cd fe b3	8a 38 75 5d 09 96 82 3f e8 fa 31 16 a2 77 ce 44 6e ac 4e 99	5f fa c4 3e 0d dc 5b 4a f2 b6 96 f6 bc 4d b7 e9 1d f3 14 bb 8f e0 d0 71 3a 0b 1a 7a d2 a6 8f ac

CN = Microsoft IT TLS CA 5
OU = Microsoft IT
O = Microsoft Corporation
L = Redmond
S = Washington
C = US
	08 88 cd 52 5f 19 24 44 4d 14 a5 82 91 de b9 52	ad 89 8a c7 3d f3 33 eb 60 ac 1f 5f c6 c4 b2 21 9d db 79 b7	f0 ee 59 14 ed 94 c7 25 2d 05 8b 4e 39 80 8a ee 6f a8 f6 2c f0 97 4f b7 d6 d2 a9 df 16 e3 a8 7f