KPMG LLP
Suite 1400
55 Second Street
San Francisco, CA 94105

## Independent Accountants' Report

The Board of Directors
Cloudflare, Inc.:

We have examined management of Cloudflare, Inc.'s ("Cloudflare") accompanying assertion that the 1.1.1.1 Public DNS Resolver service ("Public Resolver") was effectively configured to support the achievement of Cloudflare's Public Resolver commitments for the period from February 1, 2019 to October 31, 2019 ("management's assertion") based on the following criteria:

- Public Resolver data is anonymized via truncation of the source IP (truncation of the last octet for IPv4 and the last 80 bits for IPv6).
- Public Resolver data (including anonymized source IP's) is deleted from the stream processing platform within 25 hours.
- Public Resolver Logs are deleted from Cloudflare's data warehouse within 25 hours via retention configurations on the database table storing the Public Resolver Logs.
- Edge routers implemented at colocation data centers are configured to log a sample of Netflow / Sflow logging data at a sample rate of no more than .05% of all packets.
- Edge routers implemented at colocation data centers are configured to only route traffic from ports 80, 443, 853 and 53 to the Public Resolver.
- Syslog is not enabled on edge routers implemented at colocation data centers for accepted Public Resolver requests.
- System configurations supporting the Public Resolver were consistently applied for the period from February 1, 2019 to October 31, 2019.
- DNS payload information is dropped from the sampled Netflow / Sflow logging data before it is stored in Cloudflare's data warehouse.
- Netflow / Sflow sampled logging data is deleted from Cloudflare's data warehouse within 60 days.
- External access to the anonymized Public Resolver Logs in Cloudflare's data warehouse is restricted to APNIC via a unique, authorized API access key.

Cloudflare's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion that the 1.1.1.1 Public DNS Resolver was effectively configured to support the achievement of Cloudflare's Public Resolver commitments, 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.

In our opinion, management’s assertion that the 1.1.1.1 Public DNS Resolver was effectively configured to support the achievement of Cloudflare’s Public Resolver commitments for the period from February 1, 2019 to October 31, 2019, based on the criteria above, is fairly stated, in all material respects.

This report is intended solely for the information and use of Cloudflare and users of Cloudflare’s Public Resolver who have a sufficient understanding of the Public Resolver service to evaluate the sufficiency of the criteria for their intended purposes for the period from February 1, 2019 to October 31, 2019, and is not intended to be and should not be used by anyone other than the specified parties.

KPMG LLP

San Francisco, California
March 6, 2020

CLOUDFLARE

**Cloudflare, Inc.’s Assertion**

*Background*

Cloudflare, Inc. (“Cloudflare”) created a DNS resolver with the privacy and security of our users in mind. What this means is that whenever a user clicks on or types a web address in their Internet browser the resulting DNS lookup request will be sent over a secure channel to the Cloudflare Public Resolver rather than to an unknown DNS resolver that may not have clear privacy policies.

For Cloudflare’s 1.1.1.1 Public DNS Resolver service (“Public Resolver”), DNS requests enter edge routers implemented at colocation data centers worldwide. These edge routers are configured to send traffic to the Public Resolver only through restricted, predefined ports. Syslog logging is disabled for accepted traffic routed to the Public Resolver. Within the Public Resolver, the source IP address for IPv4 and/or IPv6 is truncated to anonymize the source IP address.

A log of the DNS request, with truncated source IP address, is routed from Cloudflare’s edge data centers to Cloudflare’s main data center. The data first enters a stream processing platform that translates the truncated source IP address into the autonomous system number (“ASN”) of its originating network, and deletes the data within 25 hours of ingestion. Moving from the stream processing platform, the data flows into a database table, where the DNS data record is stored with the ASN instead of the truncated source IP. The DNS data records in this database table are deleted within 25 hours.

Cloudflare’s edge routers are configured to capture Netflow and/or Sflow data, which is used to monitor network traffic volume and flows for analysis and mitigating denial of service attacks. Netflow and/or Sflow data is randomly captured from data flowing through the edge routers on a sample basis (at most .05% of packets are logged at random). The captured data does not include the payload data and is based off all network traffic entering the edge routers, which handle requests for a variety of Cloudflare services, including the Public Resolver. The Netflow and/or Sflow sampled data is routed to Cloudflare’s main data center where it is retained for no longer than 60 days. This data is not associated with DNS query information.

Cloudflare has an agreement with Asia-Pacific Network Information Centre (“APNIC”) that allows Cloudflare the use of the 1.1.1.1 IP address. In exchange, APNIC has access to the anonymized logs stored in the Public Resolver table in Cloudflare’s data center for research purposes. APNIC has access to this data through the use of a unique, authorized API key.

*Cloudflare’s Public Resolver Commitments*

The Public Resolver was designed for privacy first, and Cloudflare commits to the following:

1. Cloudflare will not sell or share Public Resolver users’ personal data with third parties or use personal data from the Public Resolver to target any user with advertisements.
2. Cloudflare will only retain or use what is being asked, not information that will identify who is asking it. Except for randomly sampled network packets captured from at most .05% of all traffic sent to Cloudflare’s network infrastructure, Cloudflare will not retain the source IP from DNS queries to the Public Resolver in non-volatile storage. These randomly sampled packets are solely used for network troubleshooting and DoS mitigation purposes.

3. A Public Resolver user’s IP address (referred to as the client or source IP address) will not be stored in non-volatile storage. Cloudflare will anonymize source IP addresses via IP truncation methods (last octet for IPv4 and last 80 bits for IPv6). Cloudflare will delete the truncated IP address within 25 hours.
4. Cloudflare will retain only the limited transaction and debug log data (“Public Resolver Logs”), set forth in Appendix A, for the legitimate operation of our Public Resolver and research purposes, and Cloudflare will delete the Public Resolver Logs within 25 hours.
5. Cloudflare will not share the Public Resolver Logs with any third parties except for APNIC pursuant to a Research Cooperative Agreement. APNIC will only have limited access to query the anonymized data in the Public Resolver Logs and conduct research related to the operation of the DNS system.

*Cloudflare’s Assertion*

Management of Cloudflare has assessed the Public Resolver service and determined that the 1.1.1.1 Public DNS Resolver service was effectively configured to support the achievement of Cloudflare’s Public Resolver commitments for the period from February 1, 2019 to October 31, 2019, based on the following criteria:

- Public Resolver data is anonymized via truncation of the source IP (truncation of the last octet for IPv4 and the last 80 bits for IPv6).
- Public Resolver data (including anonymized source IP’s) is deleted from the stream processing platform within 25 hours.
- Public Resolver Logs are deleted from Cloudflare’s data warehouse within 25 hours via retention configurations on the database table storing the Public Resolver Logs.
- Edge routers implemented at colocation data centers are configured to log a sample of Netflow / Sflow logging data at a sample rate of no more than .05% of all packets.
- Edge routers implemented at colocation data centers are configured to only route traffic from ports 80, 443, 853 and 53 to the Public Resolver.
- Syslog is not enabled on edge routers implemented at colocation data centers for accepted Public Resolver requests.
- System configurations supporting the Public Resolver were consistently applied for the period from February 1, 2019 to October 31, 2019.
- DNS payload information is dropped from the sampled Netflow / Sflow logging data before it is stored in Cloudflare's data warehouse.
- Netflow / Sflow sampled logging data is deleted from Cloudflare's data warehouse within 60 days.
- External access to the anonymized Public Resolver Logs in Cloudflare's data warehouse is restricted to APNIC via a unique, authorized API access key.

*Dane Knecht, Head of Product Strategy*  
**Cloudflare, Inc.**

**Appendix A:**

Fields captured as part of the Public Resolver Logs:

- date
- datetime
- srcAsNum
- srcIPVersion
- dstIPVersion
- dstIPv6
- dstIPv4
- dstPort
- protocol
- queryName
- queryType
- queryClass
- queryRd
- queryDo
- querySize
- queryEdns
- ednsVersion
- ednsPayload
- ednsNsid
- responseType
- responseCode
- responseSize
- responseCount
- responseTimeMs
- responseCached
- responseMinTTL
- answerData.type
- answerData.data
- validationState
- coloId (unique Cloudflare data center ID)
- metalId (unique Cloudflare server ID)

Additionally, recursive resolvers perform outgoing queries to various authoritative nameservers in the DNS hierarchy that are logged in subrequest fields. These logs are used for the operation and debugging of our public DNS resolver service.

The following subrequest data is included in the Public Resolver Logs:

- subrequest.ipv6 (authoritative nameserver)
- subrequest.ipv4 (authoritative nameserver)
- subrequest.protocol
- subrequest.durationMs
- surequest.queryName
- subrequest.queryType
- subrequest.responseCode
- subreqest.responseCount
- subreqeust.recordType
- subrequest.recordData
- subrequest.error