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

Independent Accountants' Examination Report

To the Board of Directors
Cloudflare, Inc.:

Opinion

We have examined management of Cloudflare, Inc.'s (Cloudflare) assertion (the Assertion), included in Management of Cloudflare, Inc.'s Statement on its Controls to Support the Achievement of its Public Resolver Commitments, that the controls over the configurations in the 1.1.1.1 Public DNS Resolver service (the Public Resolver) were suitably designed and operated effectively throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that the Control Objectives specified in the Assertion were achieved.

In our opinion, the Assertion is fairly stated, in all material respects.

Our opinion on the Assertion does not extend to any other information about Cloudflare's background and Cloudflare's public resolver commitments that accompanies the Assertion and our report.

Basis for opinion

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. We are required to be independent and to meet our other ethical requirements in accordance with relevant ethical requirements related to the engagement. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Intended use

The accompanying assertion by Cloudflare is based on the Control Objectives set forth therein. This report is intended for users who have reasonable knowledge of the Public Resolver to evaluate the suitability of these Control Objectives for their own purposes.

Responsibilities for the Assertion

Management of Cloudflare is responsible for:

- developing the Control Objectives as a basis for the Assertion and appropriately describing the Control Objectives;
- identifying the risks that threaten the achievement of the Control Objectives;
- designing, implementing and maintaining effective controls over the configurations in the Public Resolver to achieve the Control Objectives, and determining that the controls support the achievement of the Commitments;
- having a reasonable basis for the Assertion by performing an assessment of the suitability of the design and operating effectiveness of the controls within the Public Resolver; and
- fairly stating the Assertion.

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.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the Control Objectives are achieved. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Our responsibilities

The attestation standards established by the American Institute of Certified Public Accountants require us to:

- plan and perform the examination to obtain reasonable assurance about whether the Assertion is fairly stated, in all material respects; and
- express an opinion on the Assertion, based on our examination.

We exercised professional judgment and maintained professional skepticism throughout the engagement. We designed and performed our procedures to obtain evidence about the Assertion that is sufficient and appropriate to provide a basis for our opinion. The nature, timing, and extent of the procedures selected depended on our judgment. We identified and assessed the risks that the controls were not suitably designed or did not operate effectively to achieve the Control Objectives through understanding the Assertion and the engagement circumstances. We designed procedures that are appropriate in the circumstances to address those risks and obtain evidence about the design and effectiveness of the controls.

KPMG LLP

San Francisco, California
March 23, 2026

Management of Cloudflare, Inc.'s Statement on its Controls to Support the Achievement of its Public Resolver Commitments

Background

Cloudflare, Inc. (Cloudflare) created the 1.1.1.1 public domain name system (DNS) resolver service (the Public Resolver) with the privacy and security of its users in mind. For individuals or organizations who have configured their systems to use this service, whenever a user clicks on or types a web address in their internet browser, the resulting DNS lookup request is sent to the Public Resolver rather than to a default or unknown DNS resolver that may not have clear privacy and security policies.

For Cloudflare's Public Resolver, DNS requests enter edge routers (the Edge Routers) implemented at colocation data centers worldwide (the Colocation Data Centers). Syslog logging is disabled for accepted traffic routed to the Public Resolver. Within the Public Resolver, the user's internet protocol (IP) address (referred to as 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 the Colocation Data Centers to Cloudflare's main data centers (the Main Data Centers). The data first enters a stream processing platform that translates the truncated source IP address into the autonomous system number of its originating network.

The Edge Routers are configured to capture and monitor network traffic volume and flows for analysis and mitigating denial of service attacks using Netflow and/or sFlow network monitoring protocols. These monitoring protocols randomly capture 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 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 sampled data is routed to the Main Data Centers where it is retained for no longer than 60 days. This data is not associated with DNS query information.

Cloudflare's Public Resolver Commitments

Cloudflare has established the following commitments (the Commitments) to users of the Public Resolver:

1. Cloudflare will not sell or share the 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 the user 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 address from DNS queries to the Public Resolver in non-volatile storage. These randomly sampled packets are used for network troubleshooting and DoS mitigation purposes.

3. A Public Resolver user's 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.

Management of Cloudflare's Assertion

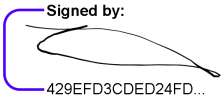
Management of Cloudflare is responsible for designing, implementing, and maintaining effective controls over the configurations in the Public Resolver to support the achievement of the Commitments.

Management of Cloudflare has evaluated whether the controls over the configurations in the Public Resolver for the period January 1, 2024 to December 31, 2024 were suitability designed and operated effectively to achieve the following control objectives (the Control Objectives):

- Public Resolver data is anonymized via truncation of the source IP address (truncation of the last octet for IPv4 and the last 80 bits for IPv6).
- The truncated source IP address is deleted within 25 hours.
- The Edge Routers implemented at the 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.
- 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, such that:
    - Logical access to system configurations supporting the Public Resolver is restricted to authorized users commensurate with job responsibilities.
    - Changes to system configurations supporting the Public Resolver are authorized, tested, and approved prior to implementation to the production environment.
- DNS payload information is dropped from the sampled Netflow / Sflow logging data before it is stored in Cloudflare's data warehouse.

Management of Cloudflare asserts that the controls over the configurations in the Public Resolver were suitably designed and operated effectively throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that the Control Objectives were achieved.

Cloudflare, Inc.



Dane Knecht

Cloudflare's Chief Technology Officer

March 23, 2026