Canadian Internet Registration Authority (CIRA) – Canadian Shield

Independent Auditor’s Report

Deloitte LLP
939 Granville Street
PO BOX 2177
Vancouver Main
Vancouver, BC V6B 3V7
Canada

Tel: 604-669-4466
www.deloitte.ca

Private and confidential
August 6, 2020

The Management of Canadian Internet Registration Authority (CIRA)

Deloitte LLP ("Deloitte" or "we" or "us") have undertaken a reasonable assurance engagement of the accompanying privacy assertions of the Canadian Internet Registration Authority ("CIRA") Canadian Shield service.

Management's Responsibility
Management is responsible for the preparation of the privacy control assertions as it relates to the delivery of the Canadian Shield service. Management is also responsible for such internal control as management determines necessary to enable the preparation of the privacy control assertions that is free from material misstatement, whether due to fraud or error.

Our Responsibility
Our responsibility is to express a reasonable assurance opinion on the subject matter information based on the evidence we have obtained. We conducted our reasonable assurance engagement in accordance with Canadian Standard on Assurance Engagements (CSAE) 3000, Attestation Engagements Other than Audits or Reviews of Historical Financial Information. This standard requires that we plan and perform this engagement to obtain reasonable assurance about whether the privacy control assertions is free from material misstatement.

Reasonable assurance is a high level of assurance, but is not a guarantee that an engagement conducted in accordance with this standard will always detect a material misstatement when it exists. Misstatements can arise from fraud or error and are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of users of our report. The nature, timing and extent of procedures selected depends on our professional judgment, including an assessment of the risks of material misstatement, whether due to fraud or error, and involves obtaining evidence about the preparation of privacy assertions in accordance with the applicable criteria.

Our engagement included procedures to assess the design of the following privacy control assertions, as at June 30, 2020:

- **C1.1:** User personal information (PI) is maintained in a secure location and only authorized system users have access to the information.

- **C2.1:** During the onboarding of a new customer of the service, users are not required to disclose personal information (PI).

- **C3.1:** During the use of the service, only the IP address and domain name queries of the user are collected by CIRA. IP addresses collected by the service attribute to a device only, and do not distinguish between single or multiple users.

- **C4.1:** User DNS query data which contains the customer's IP address is only retained by CIRA for up to twenty-four (24) hours after which the data is deleted.

Deloitte.

- **C4.2:** After twenty-four (24) hours of collecting user DNS query data, only aggregated data is retained and domain name queries cannot be attributed back to a user IP address.

- **C5.1:** In the case of malicious or anomalous activity, CIRA has the right to retain the DNS query data beyond twenty-four (24) hours to support network defense and mitigation.

- **C6.1:** Threat feeds provided by intelligence partners are utilized by the Canadian Shield system to block malicious sites. Only domain data and number of blocks associated with the domain is shared with threat intelligence partners.

- **C7.1:** CIRA shares only anonymized aggregate statistics on system service performance with the public and threat intelligence partners. This include metrics on threat type and other vertical metrics including performance of the Service (e.g. number of threats blocked, infrastructure uptime). CIRA does not share statistics that are attributable to user IP addresses.

CIRA's management is responsible for its assertion. Our responsibility is to express an opinion on whether the CIRA Canadian Shield service is suitably designed to support the achievement of management's assertion to support CIRA's commitments as at June 30, 2020, based on our examination.

Our examination was conducted in accordance with Canadian Standard on Attestation Engagements (CAEA). 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.

Limitations
Service providers were not included as part of the testing scope. No evaluation of the management controls or detailed user controls exercised by users of CIRA's services has been made. It is the responsibility of each user entity and their auditors to ensure that controls are in place at the user entity to complement the system of controls in place at CIRA.

Our Independence and Quality Control
We have complied with the relevant rules of professional conduct/code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Control 1, Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements, and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Opinion
In our opinion, management's assertion that the CIRA Canadian Shield service is suitably designed to support the achievement of CIRA's privacy commitments as at June 30, 2020, and is fairly stated, in all material respects.

Deloitte.

Restriction on use
This report is intended solely for the information and use of CIRA and users of CIRA's Canadian Shield service who have a sufficient understanding of the Canadian Shield service to evaluate the sufficiency of the criteria for their intended purposes as at June 30, 2020, and is not intended to be and should not be used by anyone other than the specified parties.

Deloitte LLP

Deloitte LLP
Vancouver, BC
August 6, 2020

Background

CIRA Canadian Shield blocks threats at the Domain Name System (DNS) level. The DNS provides the core backbone of the Internet by providing the map between easily-readable hostnames (i.e. www.cira.ca) and IP addresses (192.228.29.1). It is essential to the operation of the Internet by enabling the use of logical, human-readable names for locations rather than complex IPv4 or IPv6 addresses that computers understand. Because it is the first (invisible) step in visiting a domain name it is a perfect way to block malicious links.

CIRA Canadian Shield is, what is technically called, a policy-enabled recursive resolver. This means that it performs the functions of a recursive server in looking-up and storing the DNS information - also known as a map of the internet. However, it will not provide the answer when the site you are trying to visit is known to contain malware or phishing. Blocking it before it happens is preferable to first getting malicious code and then having it detected and cleaned by anti-virus software. You can think of it like not getting the flu at all rather than treating it with medicine after you are infected.

What does CIRA Canadian Shield do to protect privacy?

When you use CIRA it means that your prior recursive DNS resolver can no longer know and store your DNS data. Remember that the DNS is a record of all your web activity, in terms of the sites that you and your family visit. We believe that CIRA is a trusted Canadian non-profit provider of this service. We will not retain any personal information for marketing purposes and will not resell your personal data. We retain it for the shortest time possible* to deliver a quality service.

Additionally, you can use the DNS encryption (DoH) service to further protect the privacy of your DNS look-ups by encrypting the DNS queries on the internet.

CIRA's Privacy Policy

This Privacy Policy describes the policies and procedures for the Canadian Shield service (the "Service") operated by the Canadian Internet Registration Authority ("CIRA"). This Privacy Policy is incorporated into and subject to the Terms and Conditions of the Service.

a. The privacy of users of the Service is very important to CIRA. CIRA will not sell, rent, or license your personal information to any third party.

b. As an open DNS resolver, there is no signup or requirement to disclose personal information to CIRA, other than that which is provided by accessing the Service. The only method by which CIRA can identify end users is by the IP (internet protocol) address of the user.

c. When you use the Service, we collect your IP (internet protocol) address, and your domain name queries. IP addresses may represent individual persons or devices, or they may represent large groups of end users within an organization. The Service does not distinguish between single and multiple users behind a single IP address.

d. Your detailed DNS query data that includes your IP address will be retained by CIRA for up to twenty-four (24) hours, in order to identify and protect the Service from any malicious behaviour, after which time it will be deleted. Beyond 24 hours only aggregated data will be retained in which your domain name queries will no longer be attributable to your IP address.

e. In the event CIRA observes behaviours which CIRA deems to be malicious or anomalous, CIRA may retain detailed DNS query data in the course of normal network defense and mitigation. This collection will be limited to DNS query data associated with IP addresses that CIRA determines are involved in the event.

f. CIRA will use threat feeds provided by intelligence partners. CIRA may share with intelligence partners data about domains and the number of blocks associated with them. This data will not include any Canadian Shield User's Personally Identifiable Information (PII).

g. CIRA may also share high level anonymized aggregate statistics, including metrics on threat type, geolocation, as well as other vertical metrics including performance of the Service (e.g. number of threats blocked, infrastructure uptime) with the public and with its threat intelligence partners.

Management's assertion

Management of CIRA has assessed the Canadian Shield product and determined that it was effectively configured to support the achievement of CIRA's privacy control assertions as at June 30, 2020, based on the following criteria:

- **C1.1:** User personal information (PI) is maintained in a secure location and only authorized system users have access to the information.

- **C2.1:** During the onboarding of a new customer of the service, users are not required to disclose personal information (PI).

- **C3.1:** During the use of the service, only the IP address and domain name queries of the user are collected by CIRA. IP addresses collected by the service attribute to a device only, and do not distinguish between single or multiple users.

- **C4.1:** User DNS query data which contains the customer's IP address is only retained by CIRA for up to twenty-four (24) hours after which the data is deleted.

- **C4.2:** After twenty-four (24) hours of collecting user DNS query data, only aggregated data is retained and domain name queries cannot be attributed back to a user IP address.

- **C5.1:** In the case of malicious or anomalous activity, CIRA has the right to retain the DNS query data beyond twenty-four (24) hours to support network defense and mitigation.

- **C6.1:** Threat feeds provided by intelligence partners are utilized by the Canadian Shield system to block malicious sites. Only domain data and number of blocks associated with the domain is shared with threat intelligence partners.

- **C7.1:** CIRA shares only anonymized aggregate statistics on system service performance with the public and threat intelligence partners. This include metrics on threat type and other vertical metrics including performance of the Service (e.g. number of threats blocked, infrastructure uptime). CIRA does not share statistics that are attributable to user IP addresses.

_____

Dave Chiswell
Vice-President, Product
Ottawa, ON
August 6, 2020