

ccTLD DNS Abuse Survey (2026 edition)

DRAFT | open for comments

The DNS Abuse Standing Committee (DASC) is preparing to launch the **third edition of the ccNSO DNS Abuse Survey**. Before doing so, we would like to provide ccTLDs with an opportunity to review the draft questionnaire and share feedback.

Draft review period (sneak preview)

A draft version of the survey questions is now available as a PDF for review. We invite you to consult internally with relevant colleagues and submit any comments, concerns, or suggestions to ccnsossecretariat@icann.org.

- **Deadline for feedback:** 20 July 2026 (COB)

All input received will be carefully reviewed by the DASC before finalizing the survey.

WELCOME

Welcome to the 3rd survey by the ccNSO DNS Abuse Standing Committee (DASC). Conducted in August - September 2026, this survey follows up on the initial survey from Q4 2022. Read more here: <https://ccnso.icann.org/en>

DISCLAIMER

This survey is for ccTLDs only. Please submit only one (1) response per ccTLD.

Furthermore, we want to assure you that all responses collected are confidential. Your responses will be anonymized and aggregated with those of other participants to analyze trends and patterns. Any identifying information provided will be kept separate from the survey responses and will not be shared with any third parties.

The ccNSO DASC thanks you for your cooperation. If you have questions, please contact the ccNSO Secretariat at ccnsossecretariat@icann.org

1. *** I agree that my personal data will be processed in accordance with the ICANN Privacy Policy (<https://www.icann.org/privacy/policy>), and agree to abide by the website Terms of Service (<https://www.icann.org/privacy/tos>).**

Yes

2. *** I am answering this question on behalf of an organization or entity responsible for managing a ccTLD, which is listed as such in the IANA Root Zone Database.**

Yes

RESPONDENT DATA

3. *** Please specify the ccTLD(s) you represent. This also includes IDN ccTLDs. Use a comma to separate if more than one.**

4. **What is your role at the ccTLD?**

5. **We encourage you to specify your e-mail address (optional). Note that this address will not be shared with anyone, but might be used by the DASC survey team in case of questions or incomplete responses.**

6. *** Please select the ICANN geographical region for your ccTLD.**

- Africa
 Asia/Australia/Pacific
 Europe
 Latin America/Caribbean islands
 North America

7. Please select the governance model for your ccTLD.

- Academic institution
- For profit company
- Governmental institution
- Not for profit organisation
- Other (please specify)

8. Which registration model do you follow? Please select all that apply.

- 3R: Registry-Registrar-Registrant model
- Direct registrations
- Other (please specify)\

9. What is the number of domains under management for your ccTLD? Please select the appropriate range.

- 0 to 5000
- 5,001 to 70,000
- 70,001 to 50,000
- 50,001 to 100,000
- 100,001 to 1 million
- 1,000,001 to 5 million
- more than 5 million

10. How many employees (Full Time Equivalents) does your ccTLD have? Please select the appropriate range.

- 2 to 5
- 6 to 10
- 11 to 30
- 31 to 50
- more than 50

11. What is the average domain name registration price your ccTLD charges?

Price	For registrars	For the public
Less than 5 USD	<input type="checkbox"/>	<input type="checkbox"/>
Between 5 and 10 USD	<input type="checkbox"/>	<input type="checkbox"/>
Between 10 and 20 USD	<input type="checkbox"/>	<input type="checkbox"/>
Between 20 and 99 USD	<input type="checkbox"/>	<input type="checkbox"/>
More than 99 USD	<input type="checkbox"/>	<input type="checkbox"/>
Not applicable	<input type="checkbox"/>	<input type="checkbox"/>

Other (please specify)

TYPES OF ABUSES & ACTIONS

12. Which types of abuse does your ccTLD take compliance action against? Please select all that apply, and select the method of action.

Abuse Type	Proactive action (complaints/own intelligence)	Action via regulatory/enfor cement authority	Action via third-party notifications	Trigger registrant verification	none
Fake, false, incorrect registration records	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DNS Abuse (definitions SAC115. https://itp.cdn.ica.nn.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-115-en.pdf)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Financial scams / fraud	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Child Sexual Abuse Material (CSAM)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other problematic website content (e.g., hate speech, violent/extremist content, IP infringement, regulated goods)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Trademark infringement in domain name (homographs, typosquatting, cybersquatting, domain kiting, fake webshops)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

13. Approximately what % of domains in your ccTLD do you believe are subject to DNS Abuse? Please select the range that best represents your estimate.

- No measurable abuse
- Less than 0.05%
- 0.05% - 0.10%
- 0.10% - 0.15%
- 0.15% - 0.20%
- More than 0.20%
- Not sure

14. How confident are you in your answer above?

- Very confident - response is backed by data such as ICANN's Domain Abuse Activity Reporting (DAAR), NetBeacon Institute, or equivalent
- Somewhat confident - rough estimate
- Not confident

15. My ccTLD has a procedure in place for the registrant to contest or appeal ccTLD action against a domain name, for instance for DNS abuse and/or content complaints.

- Yes
- No
- Other (please specify)

16. Which of the following abuse requirements apply for registrars in your ccTLD?

- An abuse contact and/or abuse handling process is mandatory for registrars
- An abuse contact and/or abuse handling process is optional for registrars
- Not applicable (e.g., there are no registrars)
- Not sure
- Other (please specify)

17. Does your ccTLD have documentation on mitigating any of the abuse types mentioned in question 12? Please select all that apply

- Yes, we have publicly available documentation regarding the types of abusive content we are able and/or willing to take action on
- Yes, we have publicly available documentation regarding which requirements need to be met, for our ccTLD to take action against abusive domains
- We do have such documentation, but we do not publish it
- We have publicly available transparency procedures and reports
- None of the above

DETECTION

18. Malicious domains are often part of broader campaigns involving dozens or hundreds of related domains. Does your ccTLD conduct Associated Domain Checks (ADC)? ADC definition as per [GNSO's Final Issue Report \(see page 4\).](#)

- Yes, we conduct ADC regularly
- Yes, we conduct ADC occasionally (eg.on an ad-hoc basis)

- We provide reverse whois to third parties to conduct ADC. (Reverse whois is a search technique that identifies all domain names associated with a specific registrant, such as an email address, name, or organization).
- We require our registrars to conduct ADC
- None of the above

19. Domain Generation Algorithms (DGA) create large numbers of domain names, which cybercriminals use to frequently change domains and evade security tools that block known domains or IP addresses. Please select all that applies to your ccTLD.

- We have identified instances of likely DGA registrations in the past
- We are able to evidence when it is a DGA
- We actively investigate instances of likely DGAs
- Other (please specify)

20. Which methods does your ccTLD use to mitigate DNS Abuse? Please select all that apply.

- Registration Policy and/or Terms and Conditions targeting DNS Abuse
- Internal best practices
- Procedures (e.g. post-registration checks on high risk phishing terms)
- Tools (e.g. DNS detection and threat intelligence feeds)
- Consumer awareness / outreach
- Complaints procedures for third parties to report abuse
- Registrant verification procedures
- Other (please specify)

21. My ccTLD has a collaborative relationship for abuse detection with: (Please select all that apply).

- National response team, e.g. CSIRT, CIRT, CERT
- Law Enforcement Agency (LEA)
- Trusted notifier, e.g. Internet Watch Foundation
- Trademark Association
- Academic and/or Research Institution
- Industry-specific Alliance, e.g. financial services
- Legal/Judiciary/Mediation/Dispute Resolution body

- None
 Other (please specify)

22. My ccTLD entered into a Trusted Notifier arrangement (a formal agreement with a notifier) to address DNS Abuse.

- Yes
 No
 Not applicable: There is an exclusive local regulatory and enforcement authority to address a given form of abuse in my country or territory

Please explain

23. Does your ccTLD verify registrant data? Verification in this context refers to checking ID or company registration documents for instance. Please select all that apply.

	Manual verification by ccTLD	Automated verification by ccTLD	Not performed by ccTLD	Registrars are required to verify
Prior to registration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Post registration	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Upon renewal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Screening for suspicious registrations	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

24. What type of registrant information does your ccTLD validate? Validation in this context means: doing some checks to ensure the information is likely to be real.

- Name
 Address

- Phone number
- Email
- Company identifier
- Other

Please specify

25. What measures, if any, do you take to keep the domain name registration information accurate over time? Please specify.

26. My ccTLD uses the following DNS abuse feeds or threat intelligence sources. Please mark all that apply.

- Open source/community feeds (e.g. Shadowserver, SURBL, etc.)
- Commercial (e.g. Abusix, RecordedFuture, Sophos, Netcraft, .etc)
- National CSIRT/Cybersecurity centre
- None
- Other, please specify

27. If you are using DNS Abuse feeds and/or threat intelligence sources, which ones do you benefit most from and why?

28. My ccTLD uses Artificial Intelligence and/or machine learning for DNS Abuse detection and/or Intelligence.

- Yes
- No
- Not currently, but planning to
- Not sure

Please explain

MISCELLANEOUS

29. After taking action against a domain, my ccTLD continues to monitor the domain for a specific period of time to detect possible recurrence of DNS Abuse.

- Yes
- No
- Not sure

Please explain

30. My ccTLD has DNS abuse educational materials and/or carries out outreach programs to Registrars and/or Registrants.

- Yes
- No
- Not sure

Please explain

31. Overall, what are the challenges you encounter - or encountered in the past - related to the implementation of DNS Abuse Mitigation? Please specify.

32. Any final comments? Anything we forgot to ask?