## DASC survey

### 1. GENERAL

Kindly note that responses are limited to one (1) per ccTLD. Questions 1 to 4 are mandatory. The deadline for submitting your response is Friday, 15 October 2022 (23:59 UTC).

The survey contains 34 questions in total, divided over 5 phases in the domain name registration process. The estimated completion time is 10 to 15 minutes. Results will be published on the ccNSO website, however there will be an opportunity to opt-out to the publication of your ccTLD identifier. We thank you for taking the time to respond to our survey.

1 / 5 20%

* 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
- ◯ No

* 2. Please specify your ccTLD

* 3. The results of this survey will become publicly available. Please select your preferred method.

- ◯ I consent to the publication of my responses (ccTLD included)
- ◯ I consent to the anonymised publication of my responses (ccTLD will not be included)

* 4. What region are you in? Please select the ICANN geographical region for your ccTLD.

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

5. What is the governance model of your ccTLD?

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

6. Which registration model do you follow?

- ◯ 3R: Registry-Registrar-Registrant
- ◯ direct registrations
- ◯ a combination of 3R and direct registrations
- ◯ Other (please specify)

7. What is the number of registered domain names by your ccTLD? Please select a range.

- ◯ 0 to 5000
- ◯ 5,001 to 10,000
- ◯ 10,001 to 50,000
- ◯ 50,001 to 100,000
- ◯ 100,001 to 1 million
- ◯ more than 1 million

8. How many employees (Full Time Equivalents) work within the registry/registry department? Please select the appropriate range

- ◯ 1
- ◯ 2 to 5
- ◯ 6 to 10
- ◯ 11 to 30
- ◯ 31 to 50
- ◯ more than 50

9. DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS, as defined at https://dnsabuseframework.org/ Against which of these types of DNS Abuse does your registry take action? Please select all that apply.

- [ ] MALWARE Malware is malicious software, installed on a device without the user's consent, which disrupts the device's operations, gathers sensitive information, and/or gains access to private computer systems. Malware includes viruses, spyware, ransomware, and other unwanted software
- [ ] BOTNETS Botnets are collections of Internet-connected computers that have been infected with malware and commanded to perform activities under the control of a remote administrator
- [ ] PHISHING Phishing occurs when an attacker tricks a victim into revealing sensitive personal, corporate, or financial information (e.g. account numbers, login IDs, passwords), whether through sending fraudulent or 'look-alike' emails, or luring end users to copycat websites. Some phishing campaigns aim to persuade the user to install software, which is in fact malware.
- [ ] PHARMING Pharming is the redirection of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning. DNS hijacking occurs when attackers use malware to redirect victims to [the attacker's] site instead of the one initially requested. DNS poisoning causes a DNS server [or resolver] to respond with a false IP address bearing malicious code. Phishing differs from pharming in that the latter involves modifying DNS entries, while the former tricks users into entering personal information.
- [ ] SPAM Spam is unsolicited bulk email, where the recipient has not granted permission for the message to be sent, and where the message was sent as part of a larger collection of messages, all having substantively identical content
- [ ] None
- [ ] Other (please specify)

10. My ccTLD takes action against the following types of content abuse: (Please select all that apply.)

- [ ] Child sexual abuse material (CSAM)
- [ ] Cyber bullying
- [ ] Trafficking
- [ ] Illegal drugs (e.g. opiates)
- [ ] Defacement
- [ ] Terrorism
- [ ] None
- [ ] Other (Please specify)

11. My ccTLD takes action against the following types of trademark infringement: (Please select all that apply.)

- [ ] Homographs
- [ ] Typosquatting
- [ ] Fake webshops
- [ ] Cybersquatting
- [ ] None
- [ ] Other (Please specify)

12. Approximately what % of domains do you believe are subject to DNS Abuse in your ccTLD? Please select the appropriate range

- ◯ less than 0.05%
- ◯ between 0.05% and 0.1%
- ◯ between 0.1 and 0.15%
- ◯ between 0.15 and 0.20%
- ◯ more than 0.20%
- ◯ not sure

13. To mitigate DNS Abuse, my ccTLD uses the following methods: (Please select all that apply)

- ☐ Registration policies targeting DNS Abuse
- ☐ Procedures (e.g. post-registration checks on high risk phishing terms)
- ☐ Tools (e.g. DNS threat intelligence feeds & mitigation tools)
- ☐ Consumer awareness
- ☐ Complaints procedures
- ☐ None
- ☐ Other (please specify)

14. In case your ccTLDs relies on policy resources to mitigate DNS Abuse, please provide links to relevant resources and applicable sections.

15. My ccTLD has a collaborative relationship with: (Please select all that apply)

- [ ] National computer security incident response team (CSIRT)
- [ ] Law enforcement
- [ ] Trusted notifiers (e.g. Internet Watch Foundation)
- [ ] None of the above
- [ ] Other (please specify)

16. My ccTLD has an DNS Abuse Officer as part of the registry.

- ◯ Yes
- ◯ No
- ◯ Not sure

17. Data Protection legislation affects my ccTLD.

- ◯ Yes
- ◯ No
- ◯ Not sure

If you selected "yes", please specify

18. My ccTLD does outreach/education to registrars/registrants, related to DNS Abuse

- ◯ Yes
- ◯ No
- ◯ Not sure

If you selected "yes", please specify

Next

**DASC survey**

## 2. PRE-REGISTRATION

2 / 5 40%

19. My ccTLD collects the following information at the time of registration: (Please select all that applies)

- [ ] Org type (company, individual)
- [ ] Contact name
- [ ] Legal name
- [ ] Company identifier
- [ ] Email address
- [ ] Phone number
- [ ] Postal address
- [ ] Physical address
- [ ] DNS Abuse Contact

Other (please specify)

20. My ccTLD performs pre-registration verifications

- ◯ Yes
- ◯ No

21. My ccTLD validates the following information at the time of registration: (Meaning of validation in this context: doing some checks to ensure the information is likely to be real). Please select all that applies)

- [ ] Org type (company, individual)
- [ ] Contact name
- [ ] Legal name
- [ ] Company identifier
- [ ] Email address
- [ ] Phone number
- [ ] Postal address
- [ ] Physical address
- [ ] DNS Abuse contact
- [ ] None

Other (please specify)

Prev Next

**DASC survey**

## 3. POST-REGISTRATION

3 / 5 60%

22. My ccTLD uses the following methods for post-registration verifications:

- [ ] manual checks
- [ ] automated checks
- [ ] none

23. My ccTLD performs post-registration verifications:

- ◯ within 24 hours after registration
- ◯ within 48 hours after registration
- ◯ within 72 hours after registration
- ◯ never
- ◯ Other (please specify)

24. If my ccTLD detects an abuse issue, post-registration, we take the following action: (please select all that apply)

- [ ] We immediately suspend the domain name
- [ ] We immediately delete the domain name
- [ ] We give notice of suspension
- [ ] Our approach depends on the results of our risk assessment
- [ ] We take no action
- [ ] We do not have the capability to detect abuse
- [ ] Other (please specify)

Prev Next

## DASC survey

4. MID-CYCLE

4 / 5 80%

25. My ccTLD has mechanisms in place for members of the public to report DNS abuse

- ◯ Yes
- ◯ No

If you selected "yes", please specify.

26. My ccTLD entered into a Trusted Notifier arrangement to address DNS Abuse

- ◯ Yes
- ◯ No

If you selected "yes", please specify.

27. When my government or law enforcement requests a domain name take-down, my ccTLD takes the following steps:

- ◯ We execute the request without further verification from our end
- ◯ We do our own due diligence first, before considering potential actions
- ◯ Both aforementioned actions are possible
- ◯ None of the above

Other (please specify)

28. My ccTLD uses the following DNS Abuse feeds and/or threat intelligence sources: (please select all that apply)

- ☐ None
- ☐ SURBL
- ☐ Spamhaus
- ☐ Netcraft
- ☐ RecordedFuture
- ☐ Anti-Phishing Working Group (APWG)
- ☐ Sophos
- ☐ DGArchive
- ☐ Shadowserver
- ☐ Cymru
- ☐ Other (please specify)

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

30. If my ccTLD detects an abuse issue from a DNS Abuse feed, we take the following action: (please select all that apply)

- [ ] We contact the registrant/registrar, who needs to take corrective measures within a certain timeframe. If no response, we take down the domain name
- [ ] We evaluate the DNS Abuse feed, to avoid false positives
- [ ] We immediately take down the domain name
- [ ] We do not use DNS Abuse feeds
- [ ] Other (please specify)

31. What measures do you take to keep the domain name registration information accurate over time? Please specify.

Prev Next

## DASC survey

### 5. RENEWAL

5 / 5 100%

32. My ccTLD performs verifications upon renewal of the domain name

- ◯ Yes
- ◯ No

If you selected "yes", please specify.

33. If your ccTLD does not currently have any DNS Abuse processes in place, please specify when you plan to implement processes.

- ☐ within a year
- ☐ within two years
- ☐ within three years
- ☐ no plans

Other (Please specify)

34. Any final comments?