ICANN POLICY FORUM | 77
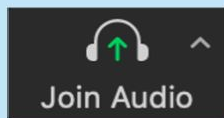
WASHINGTON, D.C.

12-15 June 2023

Virtual Participants

1

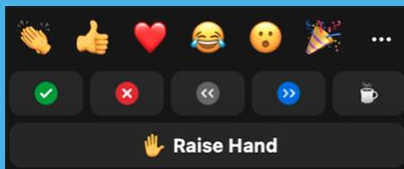Connect your **Zoom Audio** to listen to the meeting.

2

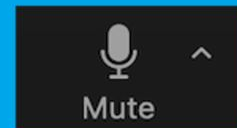Turn on your **Zoom Video** to be seen by other participants.

3

Raise your hand in **Zoom Reactions** to join the speaking queue.

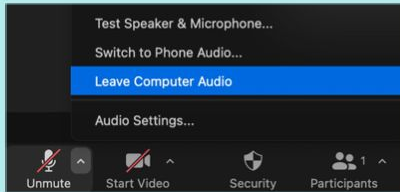**4**

Unmute your **Zoom Audio** when called upon to speak.

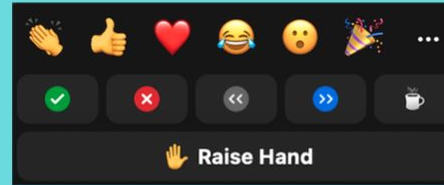# On-Site/In-Room Participants

1

Do **not** connect your **Zoom Audio**. To disconnect your audio, click on the **Up Arrow** and select **Leave Computer Audio**.

2

Raise your hand in **Zoom Reactions** to join the speaking queue.

3

Use the physical microphone at your seat or in the aisle when called upon to speak.

ccNSO DNS Abuse Standing Committee
ICANN77 | Wednesday, 14 June 2023 (13:45-15:00 local)

- Welcome & general introduction DASC
- Update by DASC Repository SubGroup
  - Launch of the repository
  - Introduction email list
- DASC Survey
  - Highlights part 1, ICANN76
  - Results part 2
  - Comparing survey results with external data
  - Pricing vs levels of abuse
  - Findings & conclusion
- What comes next?
- Final Q&A and wrap-up

ICANN | ccNSO

About the ccNSO DNS Abuse Standing Committee (DASC)

1
Share information, insights and practices

2
Raise understanding and awareness

3
Promote open and constructive dialogue

4
Assist ccTLD managers in their efforts to mitigate the impact of DNS Abuse

DASC does not formulate any policy or standards: out of scope of the ccNSO policy remit

ICANN | ccNSO

Agenda

- Welcome
- Repository subgroup milestones
- Repository library

  Background

  How to submit content

  Introduction of editorial board

- Mailing list

ICANN|ccNSO

Creation of DASC

Guest speakers

Presentation from TLD Ops

*ICANN77 - Repository launch

May 2022 | Aug 4, 2022 | Sept 2022 | Feb 2023 | June 2023 | ICANN78

First DASC Repository SG meeting

Repostory ToR submitted to Council

Email list

ICANN | ccNSO

Repository Background & Working Method:

- DASC mandate to create a dedicated resource for information sharing
- Formation/operation of a content advisory/editorial board
- Review of new content submission
- Ongoing evaluation of content for relevance and usefulness
- Editorial Board will meet 1-2x per month to review submitted content
- Community briefings

URL: https://community.icann.org/x/DoWZDg   TEMPLATE How to submit:

DASC Repository and Information Library

Created by **Kimberly Carlson**, last modified on **May 24, 2023**

The purpose of the online repository is to provide an information source created for and made available to ccTLD Managers. Content includes information relevant to the topic of DNS abuse that would be useful for such managers to identify, understand, and/or plan to take action with respect to such abuse that they may encounter.

Acceptable content

Content published on the repository must be related to DNS Abuse and relevant for ccTLDs, including, but not limited to: ccTLDs, registries/registrars, best practices, definitions

Acceptable content format: pdf, .doc, ppt, links to publications (reviewable by content board).

All contributions are welcome; however, they must observe the privacy preferences of others.

Main Categories:

- Presentations & Reports (identifying the source or event)
- Tools
- Definitions / Policies
- Articles/Commentaries

How to submit content:

Email content to **dasc-repository-submissions@icann.org**

What to include:

- *Your name:*
- *Category (presentations/reports, tools, definitions/policies, articles/commentaries:*
- *Short summary (why is this relevant/why should this be included)*
- *Source:*
- *<Include any attachments>*
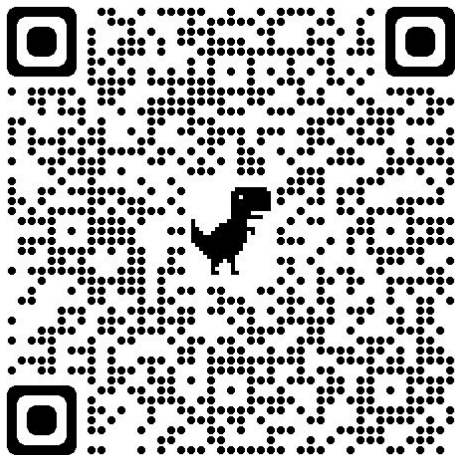- *Link to presentation:*

Process:

Once you've submitted the content, the editorial board will do the following:

1. Review the content to ensure it meets the acceptable content requirements
2. The board will determine the content's usefulness and relevance.
3. If the content meets the above criteria, the board will "accept" the content and request support to add it to the repository/library (https://community.icann.org/x/Ege7Cg)
4. The review process usually takes 14-20 working days.
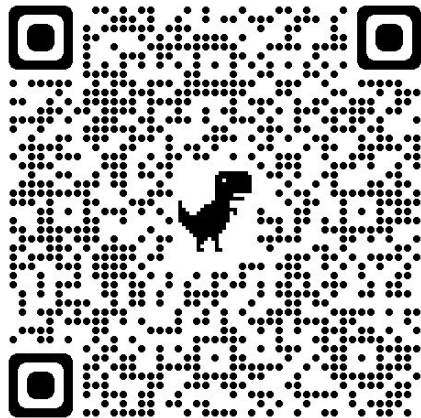
Repository and resource library

https://community.icann.org/x/Ege7Cg

ccNSO and DNS Abuse Mitigation - resource and repository

Created by Kimberly Carlson, last modified on Apr 03, 2023

The DASC Repository and Reference Library is governed by the content/editorial board (terms of reference)

Presentations & Reports

Date	Meeting	Presentation	Source
ICANN74	ICANN 74.pa DNS Abuse - 2 slides.pdf	
ICANN74	ICANN74 - .hk sharing on DN abuse v1.1.pptx	
ICANN74	ICANN74_DNS Abuse_md.pptx	
ICANN74	dns-abuse-icann74.pptx	
ICANN73	ICANN73 Roundtable Cover Slide.pdf	
	Roundtable participants	
ICANN73	ccNSO and DNS Abuse	
ICANN66	Montréal - ccNSO_ Members Meeting Day 1 (4 of 5) - PRESENTATION 2 (2).pdf	
ICANN66	DNS in times of Covid-19 ccTLD Experience.pdf	

Articles / Commentaries

Date	Presentation	Media	Comments / Notes
	Framework to Address Abuse	
	EU Study on Domain Name System (DNS) abuse	
	ICANN Org's Multifaceted Response to DNS Abuse (ICANN Blog)	
ICANN71	GAC DNS Abuse Mitigation	
	DNS Abuse Institute	
	CENTR comment on EU Study on Domain Name System (DNS) abuse	
	DAAR is Domain Abuse Activity Reporting	
30 Sep 2022	Interview with DNSAI Exec. Director	from: https://www.aei.org/

Tools

Name or Title
NetBeacon
Interisle Consulting Group's 'Phishing Landscape 2022

Definitions / Policies

| Name or Title |
|---|
| Framework to Address DNS Abuse, which has 48 registrar/registry signatories |
| Operational approaches to DNS Abuse, I&J |

Poll time (repository)

- How likely are you to visit the repository for information?
(Very Likely - Likely - Unlikely - Very Unlikely)

- Would you be interested in providing content to this repository?
(Yes - No - Maybe)

Repository Scope - Community Feedback

Meta Lawsuit Leads to Significant Decline in Phishing Domains Tied to Freenom

https://circleid.com/posts/20230527-meta-lawsuit-leads-to-significant-decline-in-phishing-domains-tied-to-freenom
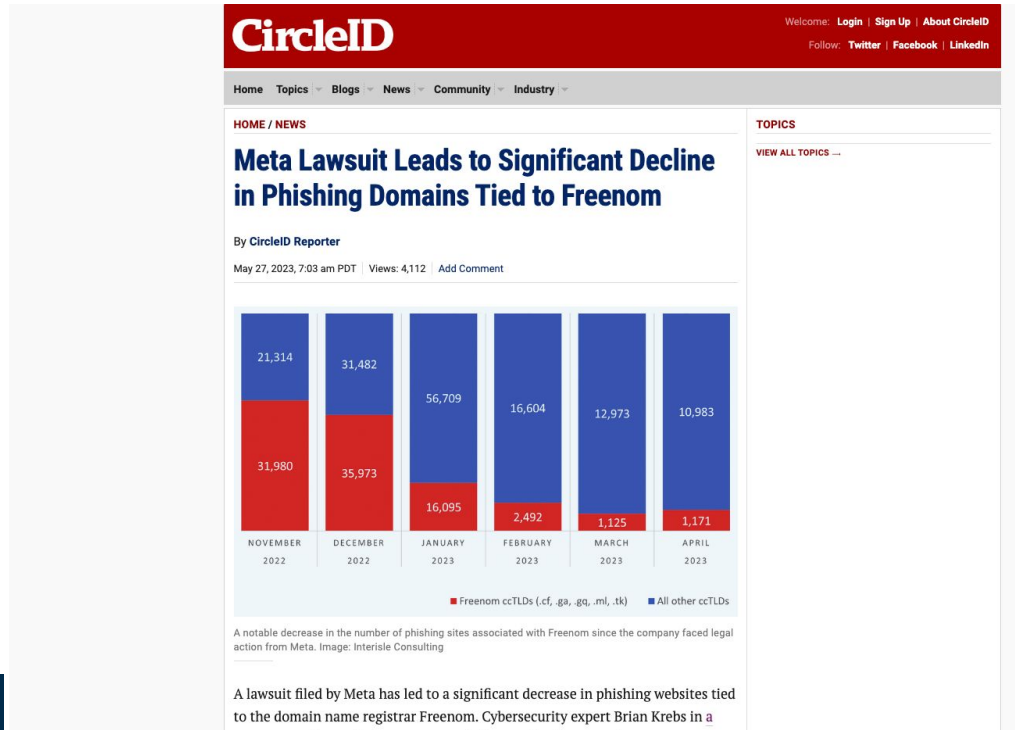
Meet the Editorial Board

- Adam Eisner
- Diego Ernesto Luna
- David McAuley
- Fernando Espana
- Jordi Iparraguirre
- Mary Uduma

Dedicated email and contact list

- Modeled after TLD Ops and other ccNSO lists
- Community list and mailing list
- Information sharing
- Closed, but not confidential
- Eligibility to subscribe to the mailing list / need to authenticate
- Monthly contact list summary

Poll time (mailing list)

- Would you be interested in subscribing to this mailing list?

  (Yes - No - Maybe)

- Are you interested in a dedicated contact list?

  (Yes - No - Maybe)

NEXT STEPS and thank you!

- Invite community to submit repository content
- Promote / word-of-mouth / share with your friends and colleagues
- Subgroup will reconvene in late June
- Complete procedural doc / concept paper
  Submit to DASC => ccNSO Council for sign-off
- Finalize logistical elements prior to launch
- Invite full DASC to subscribe and test
- Present to full community at ICANN78, invitation to subscribe

ICANN|ccNSO

About the DASC survey

Angela Matlapeng

Bruce Tonkin

Tatiana Tropina

Nick Wenban-Smith

- Open: September '22 – end November '22
- All ccTLDs were invited to respond, regardless of ccNSO membership
- 57 unique responses. Estimate: representing approx. 100 ccTLDs
  - 316 delegated ccTLDs in total (ASCII & 61 IDN alike)
  - Some ccTLD managers provide services for multiple ccTLDs, but responded for 1 TLD only
  - Some ccTLD managers informed DASC they could not respond, for various reasons
  - Some ccTLDs responded multiple times: latest submission as final one
  - Some responses were incomplete
- About half of the respondents did not want their ccTLD mentioned
- Initial report presented at ICANN76

ICANN|ccNSO

Highlights DASC survey results

part 1, ICANN76 (Cancun)

What makes ccTLDs different?

Region

Governance Model

Registry Model

% Domains Exposed to DNS Abuse

Number of Domains

Number of Employees

ccTLD has Abuse Officer

ccTLD is Affected by DPL

Highlights part 1 (continued)
See ICANN76 recordings

- Where do respondents take action?

- What are the DNS Abuse mitigation trends?

    - Mitigation methods, outreach & education to registrars

    - Trusted notifier arrangements, type of action when abuse is detected, reporting mechanisms for the public

- Tools & feeds

- Combined results: mitigation methods vs region, registry model, size

DASC survey results

part 2, ICANN77 (Washington DC)

Summary

- Pre-registration
  - Which information is being collected?
  - Do respondents perform pre-registration verifications?
  - Do respondents perform checks at time of registration, and if so, for which data?

- Post-registration
  - Methods: manual vs automated
  - When do post-registration verifications happen?

- Mid-cycle
  - Type of action when abuse is detected, based on: Feed, LEA request, due diligence verifications
  - Measures to keep registration data accurate over time

- Renewal
  - Do respondents perform verifications?

Verification: a tool to tackle DNS abuse

What do ccTLDs say?

Checks are performed:

- "within 24 h after registration and in case of complaints"
- "monthly and upon complaints"
- "when something arises"
- "upon complaint or based on random selection"
- "randomly regardless of the time of registration"

Manual and automatic verification:

- "We have a lot of manual checks of registration data. Each summer we have a lot of students helping us out with looking through data."
- "We are currently implementing a system that runs automated risk checks on newly registered domain names. We will then manually select high risk registrations for a manual verification".

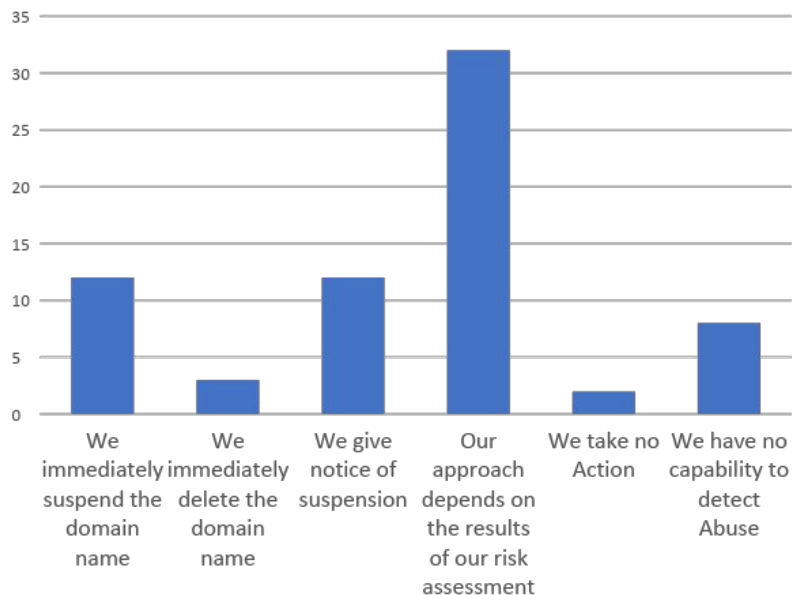# Verification: At time of registration
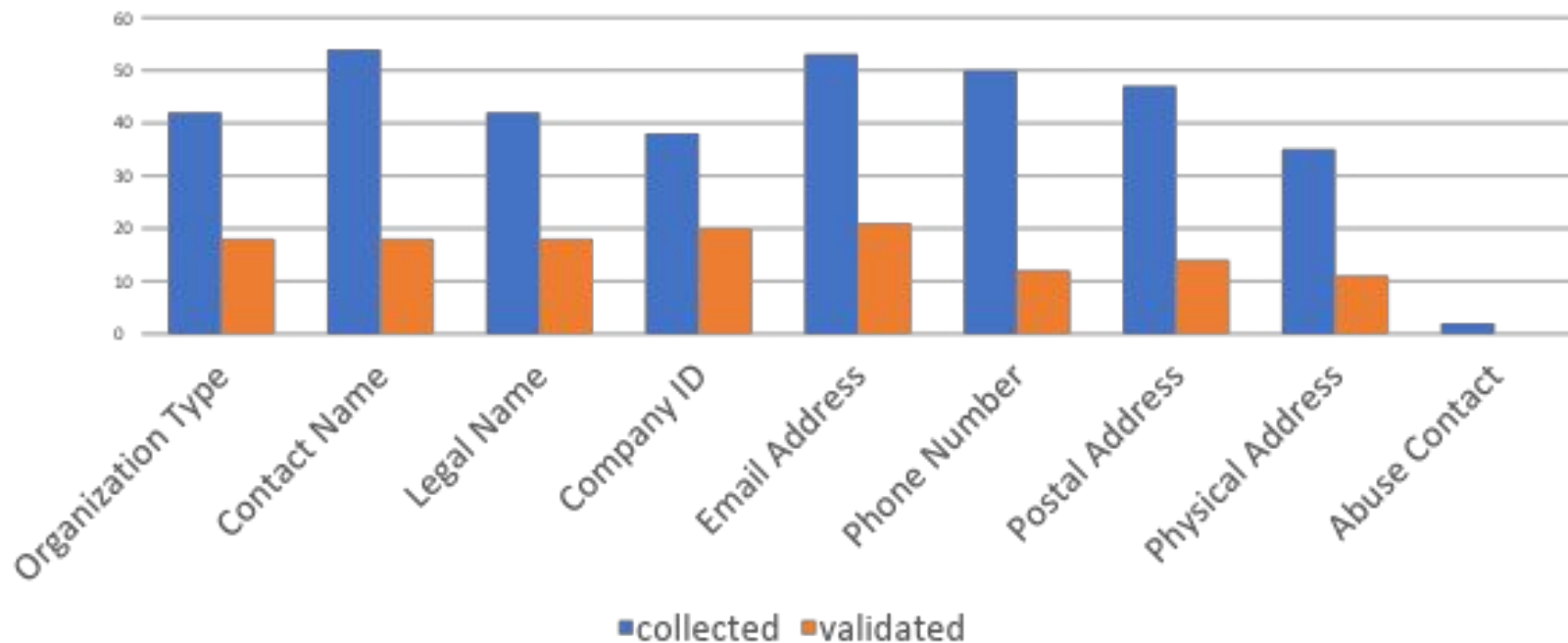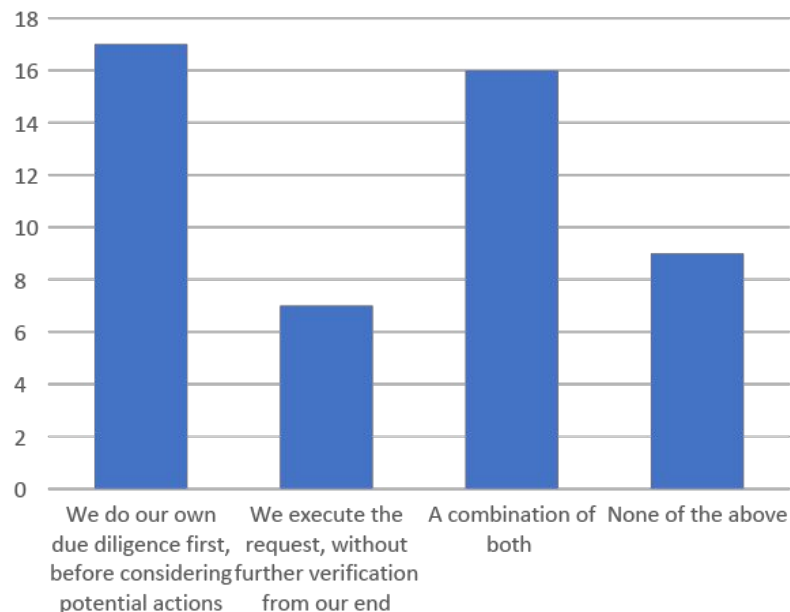
Verifications: if so, when and how?
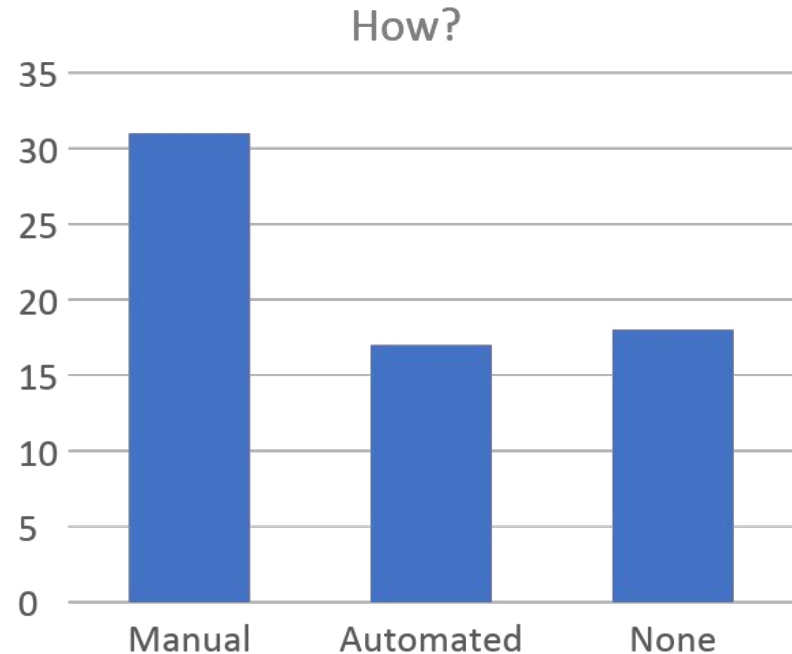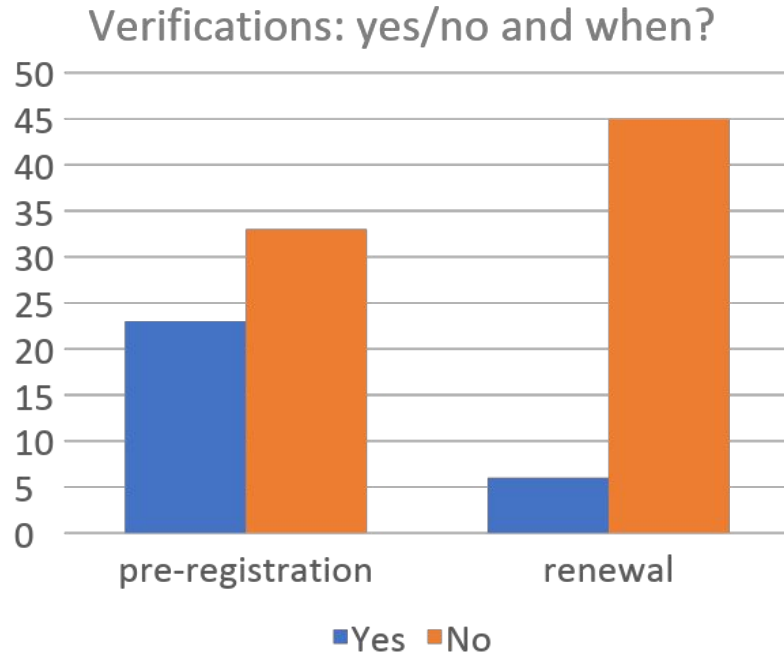
Action when abuse is detected: post-registration

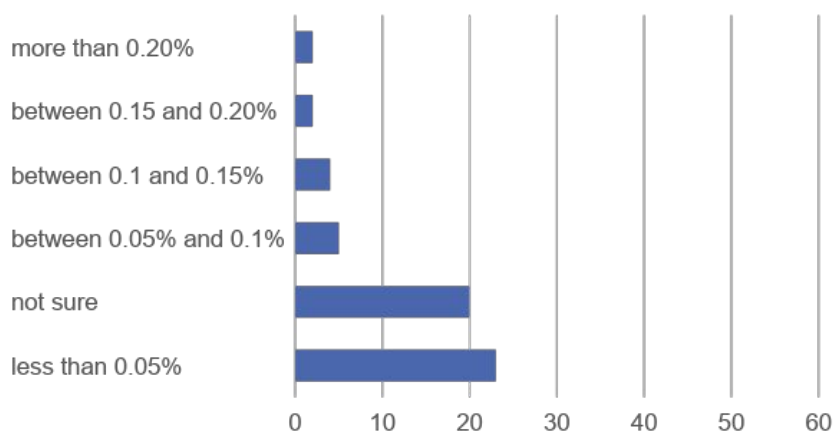Type of action

Following government request

Comparison
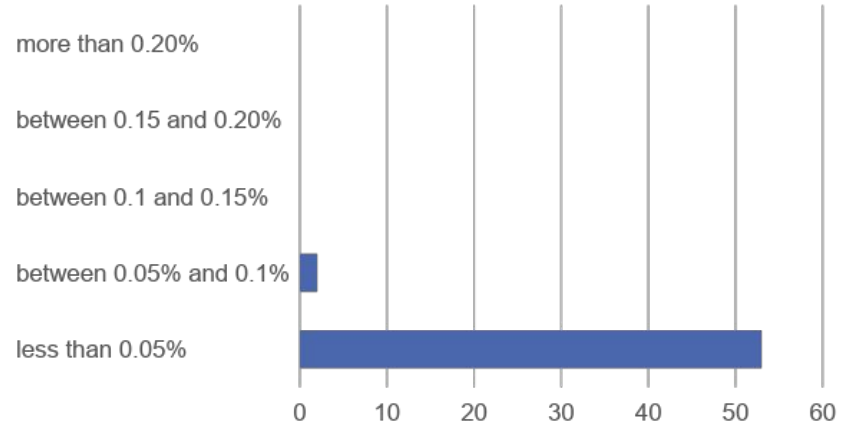
DASC survey results with DNAI data

% of domains subject to DNS Abuse

Survey - % of Domains Subject to DNS Abuse

DNS Abuse Institute: % of DNS Abuse

- Many respondents unsure about level of Abuse in their TLD. Hence, comparison with DNS Abuse Institute (DNSAI) data.
- DNSAI Compass data refers to phishing and malware only.
- Vast majority: less than 0.05% of abusive domains, less than 20 names reported as DNS Abuse.
- DNS Abuse rate of 0.05% means: only noticeable number (e.g. >100) for ccTLDs with large domain portfolio. This may explain why respondents were unsure about levels of abuse in their ccTLDs

ICANN|ccNSO

Pricing vs levels of abuse

Following up on Q&A ICANN76
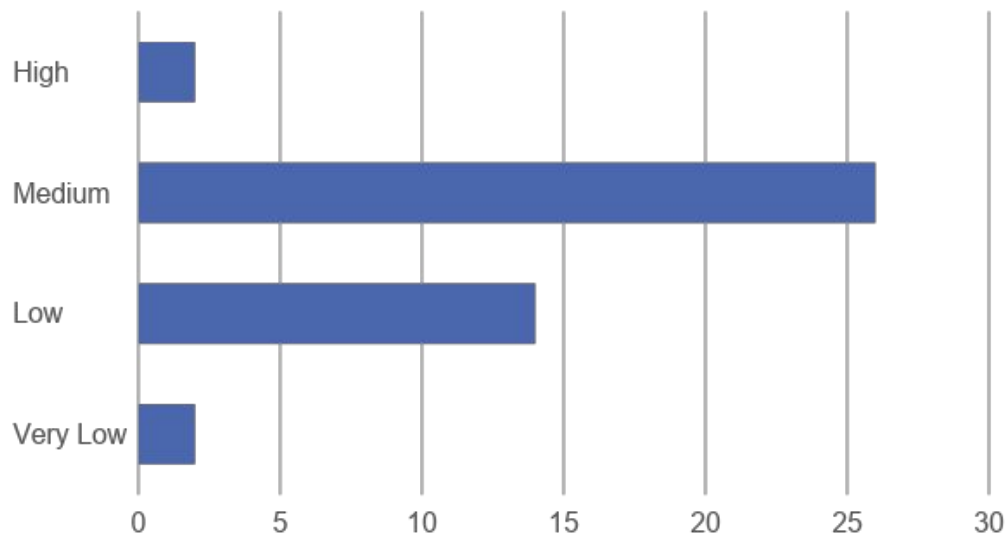
Pricing variation across ccTLDs

Legend
At retail level

High: > 100 USD
Medium: 21-99 USD
Low: 6-20 USD
Very Low: < 5 USD

- Largest ccTLDs in terms of volume of names generally in the low price range

- No discernible correlation of price with the level of DNS Abuse

- Data based on registrar and ccTLD registry pricing, where publicly available (44 ccTLDs)

ICANN|ccNSO

DASC survey Findings

- Overall, relatively low levels of abuse for ccTLDs

  - Many ccTLDs do take action, despite respondents saying they have limited resources, and do not have access to tools

  - Different types of ccTLDs do perform checks, regardless of their region, governance model, registration model, domain portfolio size, number of staff.

- Checks could happen prior to registration, but are more often done at the time of registration, or when abuse is being detected

What comes next? **Ongoing work**

- Repository
  - Manage & Expand Repository
  - Launch Email list

- DASC survey
  - Rich results, highlights presented to date: Do you want more?
  - Next DASC survey in 2024?

Poll time (survey)

- Would you be interested in a post ICANN77 webinar presenting with in-depth analyses of results ?

  (Yes - No - Maybe)

- Would you participate in a next survey in November 2025?

  (Yes - No - Maybe)

ICANN|ccNSO

What comes next? **New work items**

- Do data validation and registration policies for ccTLDs relate to DNS abuse, if so how?
- How can ccTLDs effectively work with registrars to mitigate DNS abuse?
- What are the tools and measurements ccTLDs can use to mitigate DNS abuse?
- Do ccTLD governance models and regulatory frameworks impact DNS abuse?

Poll time (new work items DASC)

- Are the proposed work items of interest to you?

  (Yes - No - Don't know - No opinion)

- What is your preferred order to hear more about the topics?

(tools and measurement- data validation and pre-registration policies - collaboration with registrars - Impact Governance Models on level of DNS Abuse - No Interest)

ICANN|ccNSO

Thank you

Next: ccTLD News Session