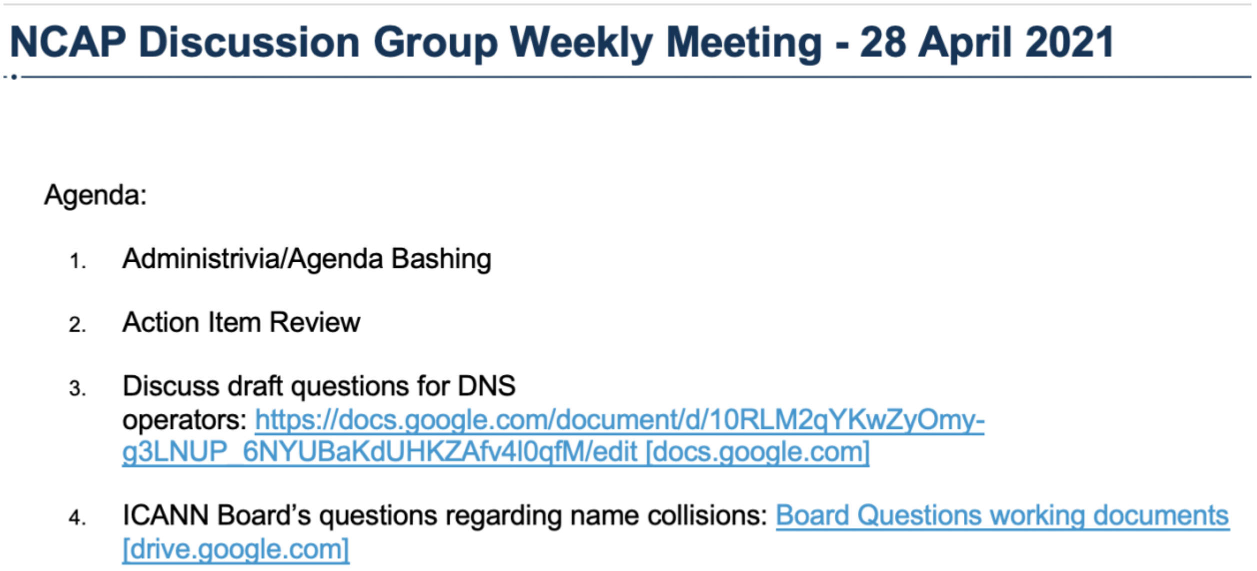

NCAP Discussion Group Weekly Meeting - 28 April 2021

Agenda:

1. Administrivia/Agenda Bashing
2. Action Item Review
3. Discuss draft questions for DNS operators: https://docs.google.com/document/d/10RLM2qYKwZyOmy-g3LNUP_6NYUBaKdUHKZAfv4l0qfM/edit [docs.google.com]
4. ICANN Board's questions regarding name collisions: Board Questions working documents [drive.google.com]

NCAP Data Questions for DNS Operators

https://docs.google.com/document/d/10RLM2qYKwZyOmy-g3LNUP_6NYUBaKdUHKZAfv4l0qfM/edit#

Reviewed Questions that Tech Analyst will ask.

These are our comments about data access are an important set of things to collect to capture rather as part of trying to do this data collection, because these are all going to feed the data sensitivity analysis, which is part of task five.

Looked at from that data, but to be honest, most of the recursive resolve operator questions that I was focusing on today is probably not likely to be answered by that data set there and we'll get into that a little bit more, as we go forward.

- For a brief period of time and then, subsequently just kind of disappear and based off of that, I think we need to consider the appropriateness of.
- 09:53If we ask group operators to do these types of measurements How important is it that the measurements are done at the roots on the same period of time.

ask that the route operator, maybe performs that analysis on their data that they contributed to the digital analysis.

for the roots it really focuses on one question, and that is how do the root letters compare to each other.

i'd like to look at and that is IP distribution overlap.

negative cash hit rate: And that is how many queries are these large open recursive resolve urs serving out of their negative cash because they've sent up a query for court and it's now caches and negative, you know, response and non existent domain and the cash.So how many of those queries are they seeing from actual clients below versus what is being sent up to the root.

Board Question #3

The harm to existing users that may occur if Collision Strings were to be delegated, including harm due to end systems no longer receiving a negative response and additional potential harm if the delegated registry accidentally or purposely exploited subsequent queries from these end systems, and any other types of harm.

https://docs.google.com/document/d/1Q6YulPRof_lsPvu3Kt0IebfOE-rr07bvICGk2dp1DNQ/edit#heading=h.z2g5jf6de200

Board Question #5

factors that affect potential success of the courses of actions to mitigate harm
https://docs.google.com/document/d/1DwHMpS-76Q_gPIKi4z5jK_V1hR6f1OzFLr7HsqnGTsU/edit#heading=h.z2g5jf6de200

question five again related mitigation question, you know how are we going to measure whether the mitigation is acting is successful or not.

And now, this is an important question when we think about mitigation, we do want to open the door for you know we know the name clinicians are going to exist. it's entirely possible that, if we can identify and characterize harm in some way, then we can have discussions about or in the future.The Board can have discussions about what kinds of things could be done to mitigate that harm. And then of course they're going to want to monitor that and we need to talk about what it means to to measure that and and determine success

how long is mitigation required? Is it possible that there's a timeline on how long you actually have to mitigate and then maybe you don't carry more and and the person who's experiencing the collision just has to make do.

Board Question #6

potential residual risks of delegating Collision Strings even after taking actions to mitigate harm

https://docs.google.com/document/d/1k2lEDN6o9TgMqjZPquRxz8mZtVLnyF-brd5nft9Zq_E/edit#heading=h.z2g5jf6de200

Barry: can't give one answer for everything, the key is looking at how well the mitigation work for this particular collision. What the scope is of it, how many how broad is the continued effect of the collision and what are the harms that are being done with this through this collision.There there absolutely may be so collisions that remain with quite a long tail that we don't really care about because the the harm is is.At an acceptable level or it has an acceptable type, but some harm that may be causing millions of dollars of damage we may have a different answer for, so I think it's it's a complicated question

Jeff: this is an academic exercise for an issue that has a slim chance of happening – we need to ensure the Board understands that so they are not reactionary.

this question is about about the long tail: what are the residual risks: one of them is making sure that we can monitor or that we get I mean potentially that we get reports. in today's model of all of this and name collisions we do a controlled interruption, and so they delegate the tld. And then you do this controlled interruption mitigation strategy at the moment, which is just a way of providing a notification to a user that something has changed. there's at least a mechanism possible for them to get more information based on having done that my the idea of getting an IP address side of things, and then they go Google that or something and and that sort of brings them to figuring out what the heck is going on.Now, whatever mitigation whatever controlled interruption becomes if it's something different, as a result of our discussion here.Once a string is delegated and you move past that step, then, rather than there being controlled interruption and.You know you have a defined response system it's now under control, the registry operator.And so the question comes, and I think this is the question you're raising and I think this is important one:

- If there's a mitigation strategy is there an obligation on the part of the Registry operator to report back on the status of that mitigation strategy?
- And then, what kind of monitoring does, I can do, of those reports and what actions would it might it take based on those reports over time?

you're not allowed to have wild cards at the end so when we begin our analysis of mitigation strategy and thinking about that we can certainly talk about this question of wild carding at that second level or not.   We will be hard pressed to create a compelling argument to allow it, given that it's been in banned.

ACTION ITEMS

#	Action Item
1	COMPLETED: Amy to research if there was any further follow-up to the letter exchange between Goran Marby and IETF regarding SAC113.

NEW QUESTIONS FOR QUESTION REGISTRY

- If there's a mitigation strategy is there an obligation on the part of the Registry operator to report back on the status of that mitigation strategy?

- And then, what kind of monitoring can you do, with those reports and what actions would be taken based on those reports over time?
- You're not allowed to have wild cards at the end so when we begin our analysis of mitigation strategy and thinking about that we can certainly talk about this question of wild carding at that second level or not? (Q6)
- kinds of harm that can occur (q6)
- Mitigation question how long is mitigation required? (Board Question 6)
- Mitigation question: how are we going to measure whether the mitigation is acting is successful or not. (Board Question 6)