NCAP Discussion Group
Meeting #66
17 November 2021 – 19:00 – 20:00 UTC

Discussion Group Members	**Observers**
Anne Aikman-Scalese, Barry Leiba, Jaap Akkerhuis, Julie Hammer, Justine Chew, Matthew Thomas, Rod Rasmussen, Warren Kumari	**ICANN Org** Matt Larson, Kathy Schnitt, Jennifer Bryce, Steve Sheng
Apologies Jim Galvin, Tom Barrett	**Contractor Support** Heather Flanagan, Casey Deccio

These high-level notes are designed to help NCAP Discussion Group members navigate through the content of the call. They are not meant to be a substitute for the recording or transcript accessed via this link: https://icann.zoom.us/rec/share/9IDgOMcDfUmqrKNWDne5FMq03lzpmuUBhFEnIa2Gatla6-Pos6hmbZ_Leql_UYgI.41B_EyNE91nCGMzv

1. **Welcome, roll call**

See attendance record above. No SOIs provided.

2. **Update from the Technical Investigator – Casey Deccio**

Casey noted that he has no further update from last week for the group.

3. **Current status of the NCAP project – Jennifer Bryce**

Jennifer noted the admin group will meet in the coming weeks to review progress and update the project plan, which will be presented to the group.

Matt Thomas provided an update on the Data Sensitivity Analysis work. He noted that initial data analysis from an open recursive resolver is underway, and he is trying to augment that with additional data from other recursive resolvers, in order to compare these against one another and against the root letters. Matt expects the Data Sensitivity Analysis to consist of two main findings at a high level:

- The first is that when you pick a letter from the root server, you will get a good high-level picture of what the root server system sees.
- That picture of the root is probably not representative of the whole bigger picture.

Further, Matt noted he is working with colleagues to develop a DNS capture extension that will run over diddle data and provide an output of the top n leaking TLDs. The hope is to eventually work with DNS-OARC to create a repository that will allow applicants to look at data in a historical context as well as the current state.

The group discussed the need to strike a balance between gathering enough recursive resolver data and deciding at some point to end data collection and focus on the report production.

4. **Name Collision Analysis – Continue discussion on the details of Step 4, particularly the basis for a honeypot**

The group discussed Heather's questions as to what "trusted third party" means (e.g. trusted by whom?) in the context of controlled interruption and honeypotting; Who is managing the honeypot? Who has access to it? Would the honeypot be something run by one of the root servers (which we're proving are equal in terms of whether the data that would come from them thanks to our sensitivity study)?

The group discussed some other questions, including:

- Technical questions around going straight to a honeypot vs. controlled interruption, for example would there be scalability issues?
- How could potential gaming be detected or accounted for in the kind of scenario of sink holing the group is discussing?
- Regarding the third party that will do the sink holing (or honey potting), and the technical review team – does the group envision these to be separate entities, or the same entity? What are their roles and responsibilities?

5. **AOB**

Matt will send an email to the group asking members to advise if they can or cannot make the scheduled meeting next Wednesday. Responses will inform if the meeting will go ahead or not.