19 July 2022

Mr. Seun Ojedeji
Chair, AFRALO

RE: AFRALO-AFRICANN ICANN73 Statement – DNS Abuse: Capacity Development for End Users

Dear Mr. Ojedeji,

Thank you for the AFRALO-AFRICANN letter regarding capacity development for end users at ICANN73. We appreciate the recommendation to focus on educating end users and raising their awareness about Domain Name System (DNS) abuse.

The ICANN Board acknowledges the thoughtful input from the AFRALO-AFRICANN community and recognizes that more work needs to be done to bring awareness regarding the active role ICANN continues to play in supporting and educating the community on DNS abuse. In response to your letter, we would like to share some highlights of recent ICANN organization-related activities which are in support of your recommendations.

The ICANN organization (org) strives to provide accurate, verifiable data, unbiased research, and expertise to facilitate fact-based discussions on the technical operations of the Internet to the entire Internet community, including end users. This includes the following activities:

- Using the data ICANN org collects and aggregates from the Domain Abuse Activity Reporting (DAAR) System, ICANN org recently published a report on DNS abuse, "The Last Four years in Retrospect: A Brief Review of DNS Abuse Trends." ICANN's DAAR project is a system for studying and reporting on domain name registration and security threats across top-level domain (TLD) registries. The overarching purpose of DAAR is to develop a robust, reliable, and reproducible methodology for analyzing security threat activity, which the ICANN community may use to make informed policy decisions. The system collects TLD zone data and complements these data sets with a large set of high-confidence Reputation Block List (RBL) security threat data feeds. We have found that the number and percentage of domains used for DNS abuse has trended downward over the last four years.

- ICANN org is planning to extend the reporting data in the DAAR project to the registrar level as part of its intention to continue to evolve DAAR. The primary impediment to implementing registrar reporting has been the consistent and dependable access to the

identifier of the registrar (registrar ID) for each domain name registration. We are pleased to report that, following discussions with the leadership of the contracted parties, we have reached an agreement to amend the Base gTLD Registry Agreement. The required change would enable ICANN org to use an existing data set provided by registries for research purposes.

- ICANN org developed the Domain Name Security Threat Information Collection and Reporting (DNSTICR) project to monitor and combat malicious online activity. It was announced via press release, to provide more information about ICANN org's increased efforts to combat Internet malware and phishing. The tool uses an evidence-based approach to identify domain names that appear to have been used for malicious purposes and are related to the COVID-19 pandemic and the Russia-Ukraine war. DNSTICR is another example of ICANN's efforts to provide accurate and unbiased data in support of mitigating Internet users from DNS security threats.

- ICANN org responded to the Call for Evidence launched by the European Commission (EC) on the European Union's (EU) Toolbox Against Counterfeiting. ICANN org's feedback was announced in April 2022 and can be found here. The contribution to the Call for Evidence is an example of ICANN org educating stakeholders about ICANN's purpose and role in making and enforcing policies that apply globally to the DNS. The EC study on DNS abuse comes at a time when this important topic is under discussion within the ICANN community.

Through ICANN Contractual Compliance, ICANN org actively enforces ICANN's policies, the Registry Agreement (RA), and the Registrar Accreditation Agreement (RAA). Below are a few examples of ICANN Contractual Compliance efforts to support combating abuse:

- ICANN org recently conducted audits specifically focused on the anti-abuse provisions for both registries and registrars. The Registrar Audit, completed in August 2021, focused on registrars' compliance with the RAA requirements related to the mitigation of DNS abuse. Like the 2019 registry DNS security threat audit, this audit further demonstrates that the contracted parties take seriously their obligations to mitigate DNS abuse.

- The blog, "New ICANN Reporting Enhances Visibility of Complaint Volumes and Trends" describes the updates made to the compliance reporting system to provide better visibility into DNS abuse complaints and others. The new reporting better captures the work of the ICANN org Contractual Compliance team and provides data that may help inform ongoing community discussions by providing more granular data on the

complaints received, the obligations enforced, and the process through which these obligations are being enforced.

- ICANN Contractual Compliance works closely with The Office of the Chief Technology Officer (OCTO) to identify DNS security threats and associate those threats with the sponsoring contracted parties. Contractual Compliance leveraged data collected by OCTO and others to proactively engage with registries and registrars responsible for a disproportionate amount of DNS security threats.

In support of your recommendation to "provide reliable DNS abuse information to the community and ensure Internet users have access to information that could benefit them, through different types of dissemination…" :

- ICANN org will continue to provide reliable DNS abuse information through blogs, announcements, press releases, webinars, and ICANN Learn so that the Internet community can easily stay informed.

- ICANN org has established the DNS Security Threat Mitigation Program, which focuses on coordinating the efforts of ICANN to mitigate DNS security threats. The program strives to make the Internet a safer place for end users by reducing the prevalence of DNS security threats across the Internet. To learn more about what ICANN is doing to help understand and mitigate DNS abuse, we encourage you to read and share with AFRALO members the program's webpage, which acts as a centralized location to find DNS security threat related information. As you'll notice, the webpage contains sections specifically dedicated to resources for end users and capacity development and training. We endeavor to make the program's webpage a resource to the community and we will continue to update it with valuable information.

In addition to the materials mentioned above, ICANN has created material for end-user DNS abuse education, specialized capacity and development training courses, awareness sessions and webinars provided by ICANN org and community members:

- ICANN continues to update and create new capacity development offerings made available through the ICANN Learn platform, which contains DNS ecosystem security offerings. DNS abuse is a key topic in these learning modules, which include practical guidance for registrants and the wider community, and share good practices to protect against malicious schemes and attacks. Specifically, the Cybersecurity Basics course on ICANN Learn provides an introduction to cybersecurity concepts and vulnerabilities that

may exist in the technologies we commonly use. You will learn about the importance of cybersecurity for end users as well as how to assess risks and protect information.

- As mentioned in its 18 May 2020 letter, ICANN org has dedicated resources for creating awareness about general DNS ecosystem security challenges, including DNS abuse. The Office of the Chief Technology Officer (OCTO) Technical Engagement (TE) and Security Stability and Resilience (SSR) teams and the Global Stakeholder Engagement (GSE) team have been providing regional webinars on related topics. The regional webinars are publicized by our Communications and GSE teams and may be of interest to end users. We invite you to visit TE's Training Course Catalog for virtual and in-person training delivered by OCTO Technical Engagement, GSE, and with community partners.

You recommend that ICANN org "create a pool of capable relevant community members and stakeholders that could provide DNS abuse awareness and education sessions to the wider Internet community." Below are a few examples of ICANN org's efforts:

- ICANN organized an "Informational Session on DNS Abuse: Panel Discussion with the ICANN Board."

- The announcement, "ICANN Launches the Special Interest Forum on Technology Discussion Platform" provided details about the new discussion platform, "Special Interest Forum on Technologies (SIFT)," that will provide the ICANN community a specific place online to discuss thematic and technical issues, and to promote knowledge sharing and discussions on the evolving Identifiers technologies and their impact on ICANN's mission. As part of the SIFT platform, ICANN is offering an active thematic SIFT on DNS abuse measurement technology with a goal to:

    - Encourage the cooperation of community members to exchange information and discuss the DNS abuse measurement technologies
    - Enable ICANN to further support the community in sharing knowledge around DNS abuse measurements
    - Present the latest developments in the Internet industry and to identify and discuss the specific issues that affect DNS abuse.

ICANN org is dedicated to understanding end user experiences through its engagement during DNS abuse related awareness sessions and webinars. As you recommend, ICANN org will listen to end users' experiences.

ICANN org is committed to do what it can, within its remit, to mitigate DNS abuse. Our intent is to continue to broaden the efforts in support of your recommendations to inform and educate end users, and strive to be recognized as a trusted source of information and to provide tools to the community for this purpose.

Together, we will continue to explore avenues in the future to promote increased awareness of DNS abuse globally. Thank you for your thoughtful letter on this important topic and we look forward to ongoing collaboration.

Sincerely,

Maarten Botterman
Chair, ICANN Board of Directors