ATTACHMENT: Highlights of ICANN org Actions to Address DNS Security Threats

ICANN org appreciates the AFRALO-AFRICANN community coming together to address this problem, highlighting relevant recommendations. ICANN org continues to take an active role in supporting the community to decide how best to address DNS Security Threats and facilitating these discussions within the community. Some highlights of our activities include:

- ICANN org has established a cross-functional program focused on coordinating the efforts of the organization related to the mitigation of DNS security threats. The program has identified several areas of focus.
- DAAR is one of these efforts. ICANN's OCTO team operates the Domain Abuse Activity Reporting (DAAR) System.
- ICANN org has dedicated resources for raising awareness about general DNS ecosystem security challenges, including DNS abuse. The Office of the Chief Technology Officer (OCTO) Technical Engagement and Security, Stability, and Resilience teams and the Global Stakeholder Engagement (GSE) team have held regional webinars on topics pertaining to DNS security threats.

Furthermore, ICANN's OCTO has implemented the following actions:

- ICANN has led over 75 technical trainings and outreach events in Africa in 2021, advancing the knowledge of threats to the DNS and mitigation strategies and recommendations, DNSSEC, network security, and resolver operations for a diverse set of audiences, including network engineers, students, policy makers, governments, trade organizations, and enterprise decision-makers.
- In November 2021, ICANN published an extensive "DNSSEC Deployment Guidebook" specifically for ccTLD operators to help reduce threats to the DNS: https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf

- ICANN developed a measurement tool to continually monitor and report threats directly associated with COVID-19-related subject matter in the DNS:
    - https://www.icann.org/en/system/files/files/octo-028-09nov21-en.pdf
- ICANN continues to iterate on the Domain Abuse Activity Reporting (DAAR) project, which measures and reports specific DNS threat models across TLD registries:
    - https://www.icann.org/octo-ssr/daar
- ICANN convened a group of world-class experts to form the DNS Security Facilitation Initiative Technical Study Group (DSGI-TSG) to investigate mechanisms to strengthen collaboration and communication on security and stability issues related to the DNS. The group's final report recommended 12 specific actions to reduce threats to the DNS for the ICANN ecosystem:
    - https://community.icann.org/display/DSFI
    - https://community.icann.org/display/DSFI/DSFI+TSG+Final+Report

In October, ICANN organized a milestone event on behalf of Afripol's and Interpol's Global Cyber Crime Directorate. The workshop enjoyed active participation by cybercrime units from 16 African countries. Presentations were given by ICANN experts, the U.S. Federal Trade Commission, the UK National Crime Agency, the national CERTs from Mauritius and Benin, the Zambian police, Interpol, the Canadian Radio-television and Telecommunications Commission, and the Global Forum on Cyber Expertise. In addition to the many DNS-related topics

discussed, special focus was given to the building of trust and the need for international collaboration to addressing threats.

- In addition, ICANN has implemented the following activities:

GDD Efforts

Global Domains Division (GDD) maintains the business relationship with gTLD registries and ICANN's accredited registrars and provides services to support them in fulfilling their contractual obligations. Through these collaborative relationships, GDD helps to combat DNS security threats and other forms of DNS abuse by connecting and coordinating activities within the contracted parties to various parts of ICANN org and the community.

Board Caucus Group on DNS Security Threat Mitigation

The Board has been engaging in multiple discussions and exploring its understanding of its role in the community's discussion and ICANN's remit when it comes to DNS abuse. As a result, the Board has decided to launch a Board Caucus Group on DNS Security Threat Mitigation to further commit re