ICANN

Washington, D.C. Engagement Center

801 17th Street, NW, Suite 400
Washington, DC 20006
USA

☎ +1 202 570 7240

+1 202 789 0104

4 April 2018

RE: Letter of 27 February 2018 from Independent Compliance Working Party

Independent Compliance Working Party
c/o Fabricio Vayara

Dear Independent Compliance Working Party:

Thank you for your letter of 27 February 2018[1] regarding DNS abuse and for meeting with us during the ICANN61 meeting in San Juan, Puerto Rico. ICANN org welcomes your willingness to collaborate to address systemic DNS infrastructure abuse. We share your optimism that, by leveraging the tools currently available under ICANN's agreements with the contracted parties, along with potential enhancements to those tools, we can make a significant dent in the unacceptably high rates of DNS infrastructure abuse.

As discussed during our meeting at ICANN61, there currently exists a large volume of spam and DNS infrastructure abuse (e.g., phishing, malware, command and control botnets) across a relatively small number of registries, registrars and registered name holders. ICANN org takes this matter of DNS infrastructure abuse seriously. The ICANN CEO has directed the Contractual Compliance department (Compliance) along with the Office of the Chief Technical Officer (OCTO) to make mitigation of DNS infrastructure abuse a high priority.

We are taking action against contracted parties with demonstrably high rates of DNS infrastructure abuse. The following describes some of the tools we use in these efforts and the challenges we face due to limitations in our contractual agreements with registries and registrars. With your help and the help of the ICANN community, we are confident that we can succeed in dramatically reducing the incidence of systemic DNS infrastructure abuse.

Ongoing efforts to combat DNS infrastructure abuse

One of the primary means available to Compliance to address DNS infrastructure abuse is through proactively auditing contracted parties. Compliance continuously performs audits to confirm that contracted parties remain compliant with all of their contractual obligations, including domain abuse handling. Concerns about DNS infrastructure abuse play a significant role in determining which contracted parties to audit. To make these selections, ICANN org relies on a handful of criteria, one of which is whether the ICANN community has raised concerns regarding contracted parties, as reflected in media reports, blogs, or inquiries/reports from community members or other contracted parties. ICANN org also reviews publicly available data, media sources and information provided by DNS reputation list providers and will, in the future, make use of data made available via DAAR after the methodology used by DAAR has been vetted by security professionals and as part of the audit selection process.

[1] The letter has been posted to the ICANN Correspondence page (https://www.icann.org/resources/pages/correspondence) with direct link at https://www.icann.org/en/system/files/correspondence/vayra-to-hedlund-27feb18-en.pdf.

As a part of the audit program, the audit team performs tests and reviews records to verify that contracted parties are compliant with the obligations. For example, for registry audits, auditors verify that registries have performed the technical analyses required by Specification 11 Section 3(b) to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets and that they have retained records of such analyses. For both registrars and registries, auditors also verify that required channels of abuse reporting are working and are being monitored. For registrars, auditors verify that the registrar have taken steps to investigate and respond to abuse complaints. Evidence of compliance could include communication records or even a suspension or deletion of a particular domain name.

To identify potential auditees with high levels of DNS infrastructure abuse, Compliance coordinates closely with OCTO. During the ICANN60 Abu Dhabi meeting, ICANN org presented the planned activities around DNS infrastructure abuse, including a demonstration of the Domain Activity & Abuse Reporting (DAAR) system. At the ICANN61 San Juan meeting, ICANN org provided an update on DAAR to the community. The tool uses publicly available feeds from organizations that track various types of abuse on the Internet. In light of ICANN org activities in DAAR, Compliance updated the audit plans with expanded questions and testing that will include use of DAAR data. Compliance continues to work with OCTO on the use of DAAR in the context of DNS infrastructure abuse issues. To address a question raised by the Working Group at our meeting concerning the submission and handling of abuse reports, please see the blog published in 2016 at https://www.icann.org/news/blog/update-on-steps-to-combat-abuse-and-illegal-activity.

Limitations in ICANN agreements with registries and registrars

As discussed during the meeting, there are potential limitations on the actions that ICANN org can take in addressing DNS infrastructure abuse. Neither the Registry Agreement (RA) nor the 2013 Registrar Accreditation Agreement (RAA) has enforceable provisions prohibiting or authorizing sanctions against systemic DNS infrastructure abuse. In addition, the RA and ICANN policies as currently defined do not authorize ICANN org to require registries to suspend or delete potentially abusive domain names. Similarly, the RAA does not authorize ICANN org to require registrars to suspend or delete potentially abusive domain names. Instead, under RAA Section 3.18, registrars are required to take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse. Registrars are also required to review well-founded reports from law enforcement and other similarly designated authorities within 24 hours of receipt. There is no requirement in the RAA that requires registrars to suspend or delete reported domains.

During our meeting in Puerto Rico, the Working Group asked whether ICANN org could rely on 2013 RAA Section 5.5 to terminate registrars with high rates of abusive domains under management. Section 5.5 enumerates the conditions under which ICANN is authorized to terminate an agreement with a registrar. Sections 5.5.2.1 and 5.5.2.1.3 authorizes a termination if the registrar:

> "5.5.2.1 is convicted by a court of competent jurisdiction of a felony or other serious offense related to financial activities, or is judged by a court of competent jurisdiction to have:
>
> 5.5.2.1.3 with actual knowledge (or through gross negligence) permitted Illegal Activity in the registration or use of domain names or in the provision to Registrar by any Registered Name Holder of inaccurate Whois information."

As this section specifies a "court of competent jurisdiction" must judge against the registrar prior to ICANN org taking action, this provision does not authorize ICANN org to terminate a registrar agreement prior to that judgment. The RAA does not authorize ICANN org to terminate the agreement on the basis of ICANN org's knowledge alone.

How you can help

While we acknowledge these potential limitations, we are seeking ways to take steps against those engaged in systemic DNS infrastructure abuse. We would like you to help us identify ways to approach these efforts within the limitations of our agreements. For example, we would welcome your views on how we might interpret these agreements in a manner that would allow us to pursue those engaged in systemic DNS infrastructure abuse more aggressively. As mentioned during our meeting, we would also welcome any data that will lead to evidence of DNS infrastructure abuse and enforcement.

Transparency is an important component in our efforts to address DNS infrastructure abuse. In the past year, Compliance enhanced the reporting transparency on the subject matter of complaints related to Abuse as well as WHOIS Inaccuracy, Transfer, GAC Category 1 Safeguards and Public Interest Commitments. The enhanced reports provide the community with further insight into the complaints from receipt to closure. We are continuously looking for additional opportunities to enhance transparency, particularly around DNS infrastructure abuse. We would be grateful for any ideas you may have that could at least provide greater clarity to the community as to the perpetrators, their methods and potential tools that might mitigate against

Finally, to help raise community awareness of these issues, we would also encourage you to participate in discussions facilitated by the Consumer Safeguards department. ICANN org's Consumer Safeguards efforts focus on generating and facilitating community-wide discussions about the effectiveness of existing safeguards whether additional safeguards are appropriate to address matters within ICANN's scope and remit. These discussions could in turn lead to community policy development efforts to adopt new safeguards specifically targeted at DNS infrastructure abuse mitigation. They could also potentially lead to enhancements to the agreements with registries and registrars.

We look forward to continuing to engage with you and the ICANN community on this very important matter.

Sincerely,

Jamie Hedlund
Senior Vice President, Contractual Compliance and Consumer Safeguards,
Managing Director - Washington, DC office