ICANN

The Internet Corporation for Assigned Names and Numbers

8 February 2017

Mr. Thomas Schneider
Chair, ICANN Governmental Advisory Committee (GAC)

Re: Annex 1 to GAC Hyderabad Communique

Dear Mr. Schneider:

I am writing in regards to the Hyderabad Communiqué published on 8 November 2016.[1] In Annex 1: Questions to the ICANN Board on DNS Abuse Mitigation by ICANN and Contracted Parties, the GAC posed a series of questions relating to the implementation of the Registrar Accreditation Agreement, the implementation of the Registry Agreement, DNS abuse, and other subjects.

Attached to this letter, you will find the ICANN organization's responses to the GAC's questions.

ICANN thanks the GAC for its attention to these important topics. We look forward to continuing our dialogue on these subjects.

Sincerely,

Göran Marby
President & CEO, ICANN

[1] *See* *https://www.icann.org/en/system/files/correspondence/gac-to-icann-08nov16-en.pdf*

ANNEX 1 TO GAC HYDERABAD COMMUNIQUE

Questions to the ICANN Board on DNS Abuse Mitigation by ICANN and Contracted Parties

ICANN's responses are in blue.

I. Implementation of 2013 RAA provisions and Registrars Accreditation

1. WHOIS Accuracy Program Specification - Cross Validation Requirement
   What is the implementation status of the 2013 RAA, WHOIS Accuracy Program Specification, Section 1 (e) which provides that Registrar will "*Validate that all postal address fields are consistent across fields (for example: street exists in city, city exists in state/province, city matches postal code) where such information is technically and commercially feasible for the applicable country or territory*"? Specifically, ICANN should provide:
   a. Detailed information on what registrars and ICANN have done to fulfill this RAA requirement to date;
   b. A timeline with specific milestones & dates, including a projected closure date for complete implementation of this requirement;
   c. Detailed information on cross-field validation software, approaches, etc. that have been considered, including supporting data and research;
   d. Detailed information regarding registrars' concerns about why specific options are not technically and commercially feasible, including supporting data and research; and
   e. Current proposals for cross-field validation (published at the time they are shared with any registrar).

   In mid-2014, ICANN Org and the Registrar Stakeholder Group jointly agreed to place on hold the across field validation initiative specified in Section 1(e) of the WHOIS Accuracy Program Specification to the 2013 Registrar Accreditation Agreement. This initiative was placed on hold due to the implementation of the domain verification and suspension requirement outlined in the WHOIS Accuracy Program Specification. Registrars were challenged with maintaining parallel tracks as it pertained to these two initiatives. Over the course of the last three years, ICANN Org has focused its efforts on identifying commercially reasonable and global solutions that would meet the requirements of the RAA as well as regional and global addressing and data format requirements. During ICANN57 in Hyderabad, India, ICANN Org presented the results of this research in an open session, as well as a strawman proposal to address this issue.

   In January 2017, the WHOIS Validation Working Group was re-formed to focus its effort on identifying, specifying, and approving (by a minimum of two-thirds (2/3) vote of the Registrar WHOIS Validation Working Group), an appropriate set of tools to enable registrars to complete the across field address validation specified in Section 1(e) of the WHOIS

Accuracy Program Specification of the 2013 Registrar Accreditation Agreement. Starting in the first quarter of 2017, the Working Group and ICANN Org plan to define and mutually agree upon the ability to determine if a solution(s) is commercially viable, based on provider criteria that will be drafted and agreed upon by Working Group and ICANN Org.

A complete set of documents is located on the Across Field Address Validation Wiki Page: https://community.icann.org/display/AFAV/Registrar+Across+Field+Address+Validation

The Wiki page also includes details of potential commercially reasonable solutions that the Working Group will evaluate and analyze in conjunction with ICANN Org.

2. Enforcement by ICANN of WHOIS Verification, Validation and Accuracy Requirements
Per the 2013 RAA WHOIS Specification, how does ICANN enforce all registrar WHOIS verification, validation and accuracy contractual obligations? Please provide examples that demonstrate how ICANN is enforcing each of these contractual obligations?

ICANN Contractual Compliance monitors and ensures compliance with the verification, validation, and accuracy requirements of Section 3.7.8 of the 2013 RAA and the WHOIS Accuracy Program Specification (WAPS) through:

- Processing WHOIS inaccuracy complaints covering verification, validation, and investigation and correction of accuracy issues. Between November 2015 and November 2016, WHOIS inaccuracy complaints constituted approximately 70% of complaints processed by ICANN Contractual Compliance (almost 32,000 complaints).
- Performance of the ICANN Contractual Compliance registrar audit, which includes WHOIS data verification and validation requirements.
- Processing the WHOIS Accuracy Reporting System (ARS) inaccuracy reports. The ARS checks samples of WHOIS contact information format (syntax) and functionality (operability) for accuracy from across the gTLDs. The data is provided to ICANN Contractual Compliance for follow-up with registrars (including WHOIS inaccuracy complaints and registrar outreach).
- Proactive monitoring and outreach by ICANN Contractual Compliance.

Enforcement of Section 3.7.8: This section requires registrars to take reasonable steps to investigate and correct WHOIS data inaccuracies. Per contract, Registrars have 15 calendar days after trigger event (for example: new registrations, inbound transfers, change to registrant information, WHOIS Inaccuracy complaints) to verify/validate, as applicable. ICANN enforces the obligation by requesting:

1. Evidence such as when, how, and with whom communication was conducted
2. Validation of any data updated following investigations
3. Verification of registrant email per Section 4 of WAPS

ICANN looks for one of three results when reviewing WHOIS inaccuracy complaints:

1. WHOIS updated within 15 days of notifying the Registered Name Holder – registrar provided documentation of validation of updates and verification (including affirmative response or manual verification)
2. No response from Registered Name Holder within 15 days of notifying Registered Name Holder – domain suspended until registrar has verified information
3. WHOIS verified as accurate (no change) within 15 days of notifying Registered Name Holder – registrar provided documentation of verification

ICANN may also request evidence of WAPS fulfillment under Section 1.

3. Diligence by ICANN in Relation to Registrars' Duty to Investigate Reports of Abuse
What is the standard of diligence that ICANN applies to registrars in the registrar's duty to respond to reports of abuse according to Section 3.18 of the 2013 RAA?

ICANN Contractual Compliance monitors compliance with Section 3.18 of the 2013 RAA through:

- Processing abuse complaints submitted through the Registrar Standards Complaint Form (https://forms.icann.org/en/resources/compliance/complaints/registrars/standards-complaint-form).
- Conducting the Registrar Audit Program which includes the obligations of Sections 3.18.1, 3.18.2, and 3.18.3 of the 2013 RAA.

For abuse complaints, ICANN confirms that the reporter sent abuse report(s) to registrar abuse contact email address before ICANN sends complaint to registrar. Once confirmed, ICANN could request the registrar to provide:

1. A description of the steps taken to investigate and respond to abuse report
2. The amount of time taken to respond to abuse report
3. All correspondence with complainant and registrant
4. The link to website's abuse contact email and handling procedure
5. The location of dedicated abuse email and telephone for law-enforcement reports
6. The Registrar's WHOIS abuse contacts, email address, and phone number
7. Examples of steps that registrars have taken to investigate and respond to abuse reports include:

    a. Contacting the registrant
    b. Requesting and obtaining evidence or licenses
    c. Providing hosting provider information to complainant
    d. Performing WHOIS verification

e. Performing transfer upon request of registrant
f. Suspending domain

4. Awareness Efforts by ICANN on Registrars' Obligations:
What efforts does ICANN undertake to ensure registrars, are educated and aware of their contractual obligations? Per 2013 RAA, Section 3.13, can ICANN provide details of required training, for instance:
a. Is there an ICANN training program with corresponding links and information?
b. How often is this training provided?
c. Other details of the training program?

Yes. ICANN has developed a training program in collaboration with the registrar community. The program is intended to help ICANN-accredited registrars understand and comply with their obligations under the Registrar Accreditation Agreement and incorporated consensus policies. The training is available on the ICANN Learn training platform: https://www.icann.org/resources/pages/registrar-training-resources-2015-09-23-en.

The training is web-based and can be accessed at any time upon successful account creation and login. Section 3.13 of the 2013 RAA requires the primary contact or designee to complete a training course covering registrar obligations under ICANN policies and agreements. A Certificate of Registrar Training Course Completion is published at https://www.icann.org/resources/pages/registrar-training-resources-2015-09-23-en.

Registrars are required to send in a signed and dated copy of the certificate upon successful completion of the training program.

In addition, ICANN conducts outreach to contracted parties at ICANN public meetings, GDD Industry Summits, via a webinar-type approach, or through published material on ICANN.org. The outreach provides overall contractual guidelines, informs of policy and/or contract changes, and provides an opportunity to proactively collaborate and address compliance issues.

5. Vetting Registrar Accreditation Applications
ICANN has listed criteria for registrar accreditation. Please explain how these criteria have been put into practice and enforced? Specifically:
a. How does ICANN verify information provided in registrar accreditation applications? What databases, record checks, etc. are used?
b. How many applications has ICANN received since the new process began? Of those, how many applications have been rejected, why?
c. How long does it take ICANN to evaluate each application?
d. What are the financial costs associated with processing each application, including verification costs?

ICANN conducts a thorough review of applications for Registrar Accreditation. This review includes, but is not limited to:

- Background checks conducted through a third-party service provider, Thomson Reuters. These checks include: Litigation, Bankruptcy, Regulatory, and Law Enforcement checks, as well as internet searches.
- Financial review; a review of financial statements and bank verification
- Review of good standing documents, e.g., Certificates of Incorporation, Business Registration/License
- ICANN Contractual Compliance status

ICANN has received a total of 2,157 applications in calendar years 2012 through 2016, four of which were withdrawn and eleven of which were rejected. Reasons for rejection included background check findings, financial review findings (such as insufficient cash on hand), and application review findings.

Table 1. Registrar Accreditation Applications, 2012 - 2016

Year	**Applications**	**Withdrawals**	**Rejections**
2012	57	0	6
2013	183	2	3
2014	519	1	1
2015	847	1	1
2016	551	0	0
Total	**2157**	**4**	**11**

Review of Registrar Accreditation Applications take on average three to six months. However, this timing is largely dependent upon the responsiveness of the applicant. Delays in applicant response may extend the overall review cycle to twelve months or longer.

II. Implementation of New gTLD Applicant Guidebook and Registry Agreement

1. Vetting Registry Accreditation Applications

The New gTLD Applicant Guidebook[7] (v. 2012-06-04), Module 1, Section 1.2.1, Eligibility states that "*ICANN will perform background screening in only two areas: (1) General business diligence and criminal history; and (2) History of cybersquatting behavior*." How is ICANN monitoring, enforcing and/or verifying continued compliance with Section 1.2.1?

The Applicant Guidebook requirements were used to evaluate the applicants.

ICANN monitors, enforces, and/or verifies continued compliance via Article 1.3.a Representations and Warranties in the New gTLD Registry Agreement, which covers continued compliance with what an applicant stated in its application. ICANN monitors media reports including social media, reviews complaints received and the registry's annual certification where applicable, and conducts audits addressing these issues. Verifying compliance may include requesting different types of documents such as current Certificate of Subsistence (also known as "Good Standing Certificate") or the local equivalent, and recent fiscal year Financial / Operational Statement or the local equivalent (audited, if available with redacted proprietary or confidential data).

2. Security Checks, Specification 11, Section 3(b)

a. Does ICANN collect and/or review these statistical reports or otherwise verify that the Public Interest Commitment is being met?

Specification 11 in the New gTLD Registry Agreement enables ICANN to request reports related to the Security Checks undertaken by Registry Operators and the actions taken to address them. ICANN reviews each report individually to address a reported issue; this is a proactive review initiated as a result of monitoring or an audit.

Statistical reports most commonly include:

- Number of domain names reviewed during analysis
- List of domain names with potential threats
- Type of the threat identified - malware, botnets
- Type of actions taken in response to threats
- Status (open/pending/closed) and statistics on actions taken
- Additional details on threats such as IP address, geographic location, and registrant information
- Trends and alerts

b. Is ICANN conducting any type of independent research that allows it to obtain metrics and generate statistics related to concentration of malicious domain names per registrar/registry and how this trends over a determined period of time?

At this time, ICANN is not generating statistics on malicious domains in a comprehensive way. However, the Office of the Chief Technology Officer is conducting a research project that works with industry experts to develop a service that consolidates a number of DNS abuse-related data feeds to generate statistics on a variety of malicious domain names per registrar and registry. The intent of this research project is to provide an authoritative, unbiased, and reproducible data set that tracks DNS abuse-related trends over time.

c. If ICANN is conducting this research, please provide a brief explanation of how the analysis is performed and what specific actions ICANN takes in response to the results indicated by the data.

As mentioned in response 2b, there is a research project in development. The analysis being performed is to aggregate data feeds and generate an index based on the prevalence of the different kinds of abuse that are being reported. While ICANN's plans regarding actions with the data have not yet been finalized, it is likely those actions will include at least informing registries and registrars of their abuse statistics and their position relative to the median for the industry, and working with the organizations that request ICANN's help in mitigating the abuse.

d. If ICANN is NOT conducting this research, please explain why not. In the interests of transparency, the GAC requests a report containing these statistics and summaries of actions taken in response to the security threats identified above.

At this point in time, the tool used to aggregate and report on DNS abuse is still under development. The current plan is to have the tool in beta by the second quarter of 2017.

e. The GAC would like to remind ICANN that the list of Security Threats in the New gTLD Safeguards is not meant to be exhaustive. In fact, the Security checks Safeguard applicable to all New gTLDs refers to "*security threats such as phishing, pharming, malware, and botnets*" (emphasis added), which does not exclude other relevant threats. Please describe what analysis and reporting is conducted regarding other relevant threats not listed above, including spam?

The tool being developed is limited to the data we can collect from the various malicious domain name-related services such as SURBL, Spamhouse, etc. At this time, the data available allows us to aggregate information relating to malware, botnet command and control, phishing, and spam. As more forms of abuse are provided via data feeds we can gain access to, the tool will be modified as appropriate.

3. <u>Awareness Efforts by ICANN on Registries' Obligations</u>:
What efforts does ICANN undertake to ensure registries, are educated and aware of their contractual obligations? Is there an ICANN training program with corresponding links and information?

ICANN conducts outreach to contracted parties at ICANN public meetings, GDD Industry Summits, via \webinarh, and through published material on ICANN.org. The outreach provides overall contractual guidelines, informs of policy and/or contract changes, and provides an opportunity to proactively collaborate and address compliance issues.

In addition to the ongoing efforts outlined above, in 2014, ICANN's Global Domains Division conducted a series of global, interactive, hands-on workshops designed to provide guidance to Registry Operators, Registry Back-end Technical Operators, and Agents of Registries.

III. DNS Abuse Investigation, reporting and mitigation performance

1. Abuse Investigations, Research, Reports
ICANN's IS-SSR programs are an internal resource that could be utilized for contract enforcement purposes. In addition to ICANN's IS-SSR programs, there are several publically available anti-abuse reports that can be used to assist ICANN in enforcing contractual obligations with gTLD registries and registrars.

a) Is ICANN contract compliance staff aware of such publically available abuse reports?

I. If so, does ICANN utilize these to assist in contract enforcement?
II. If ICANN utilizes such publicly available abuse reports for contract enforcement purposes, how does it utilize such reports?
III. Identify what reports or sources ICANN utilizes?
IV. If ICANN does *not* utilize these reports for contract enforcement purposes, is there any reason why not to? Are there any plans or a willingness to do so in the future?

b) Does ICANN have any intention to utilize its IS-SSR programs for contract enforcement purposes?

I. If so, how?
II. If not, why not?
III. Has ICANN's IS-SSR considered establishing a baseline for good registry and registrar behavior? If so, please provide details.

Regarding questions III.1.a and III.1.b, ICANN's Contractual Compliance Approach and Process includes monitoring activities that are ICANN-initiated, based in part on industry articles and trend analysis. This includes publicly available anti-abuse reports and ICANN-generated reports. These reports may be used for Compliance review and action to the extent that the reports cover topics that are within the scope of the 2013 Registrar Accreditation Agreement and Registry Agreement. In addition, these reports are one part of the selection criteria for the registrar and registry audit programs.

2. Multi-Jurisdictional Abuse Reporting
ICANN's former Chief Contract Compliance Officer, Allan Grogan, published a blog post on 1 October 2015 entitled "*Update on Steps to Combat Abuse and Illegal Activity*". In this blog post, Mr. Grogan indicates the complainant must identify the law/regulation violated and

the applicable jurisdiction. Many cyber/malware/botnet attacks affect many TLDs spread across many international jurisdictions.

a) Please clarify what procedures should be followed when a complainant seeks to submit valid reports of abuse to registrars involving incidents in multiple jurisdictions?
b) In particular, what does ICANN require from complainants to identify those laws/regulations in the jurisdictions of each affected registrar?

Reporters should provide as much information as possible when submitting a complaint, including information regarding alleged violations of laws/regulations in one or more applicable jurisdictions.

As stated in the blog, ICANN Contractual Compliance considers it reasonable for a registrar to expect that a report of abuse or illegal activity should meet at least the following criteria, absent extenuating circumstances or reasonable justification:

1. The complaining party should be identified in the abuse report and should provide a way for the registrar to contact the complaining party.
2. The specific url(s) that are alleged to be the source of the abuse or illegal activity should be identified, i.e., the registrar should not have to guess or search the website to understand where the offending material is located or offending activities are being conducted.
3. The nature of the alleged abuse or illegal activity should be identified with specificity, including identification of the relevant law or regulation alleged to be violated and the applicable jurisdiction where such law or regulation is in effect.
4. If the complaint alleges infringement or violation of an individual or entity's rights under a law or regulation, the report should identify the individual or entity whose rights are alleged to be violated or infringed, and the relationship between the complaining party and such rights holder (e.g., is the complaining party the individual or entity whose rights are alleged to be violated or infringed, or an authorized agent of that party or is there some other relationship).
5. If a court, regulatory authority, or law enforcement agency has made a formal determination that abuse or illegal activity is taking place, that formal determination should be submitted if available.
6. If the abuse report requests the registrar's compliance with a particular law or regulation, it should set forth the basis for believing that the registrar is subject to that law or regulation.
7. A complaining party should not submit multiple abuse reports complaining about the same instance of the same activity if the registrar has previously responded to an abuse report about that activity.

ICANN requires sufficient information to enable ICANN and the registrar to review and determine a proper response or action in relation to the alleged violation of law or regulation for the applicable jurisdiction(s).