==========

From: Donna Aust n
Date: 11/19/2018
To: ICANN Comp a nts Off ce
Subject: ICANN the company and/or a department w th n ICANN

Dear ICANN Comp a nts Off cer,

The Reg str es Stakeho der Group (RySG) s f ng th s comp a nt (Comp a nt) regard ng the recent Request For Informat on Aud t Request (RFI) ssued by ICANN Contractua Comp ance (Comp ance) to a Reg str es.

The RySG cons ders many of the quest ons nc uded n the RFI to be:

(1) outs de ICANN's aud t r ghts as set forth n the respect ve Reg stry Agreements (RAs);
(2) not ta ored to assess comp ance w th ob gat ons conta ned n the RAs; and
(3) ref ect an expans ve v ew of Comp ance's m ss on.

The RySG ra sed these concerns d rect y w th Comp ance on severa occas ons, and requested that quest ons that are out of scope of an aud t be removed from the RFI or that each quest on be t ed to a contractua c ause.

Comp ance s not w ng to remove the out of scope quest ons from the RFI, or t e each quest on to the spec f c contractua c ause to wh ch t perta ns. Therefore, the RySG s seek ng the ass stance of the Comp a nts Off ce. The RySG respectfu y requests that the Comp a nts Off cer rev ew the attached and take act on n the form of gu dance to ICANN Org that the RFI conta ns quest ons outs de the rem t of contractua aud ts as def ned n each RA.

G ven the mpend ng dead ne and genera t m ng assoc ated w th the Comp ance reg stry aud t, we respectfu y request that th s Comp a nt be dea t w th n a t me y manner.

Donna Aust n
Cha r, RySG

ref:_00D1aY7OU._5001Pn2ASM:ref

RySG Complaint - November 2018 Registry Audit

Background and Timeline

On 10 October 2018, ICANN Compliance sent a notice to Registry Operators stating that an audit was forthcoming. On 29 October 2018, following conversations between individual registries and Compliance staff members, as well as discussion and a request made during the RySG meeting at ICANN63, Compliance provided Registries with the Request For Information (RFI) questions in advance of the audit commencing.

On 2 November 2018, the Chair of the RySG wrote to Jamie Hedlund and Maguy Serad raising concerns about the breadth of the audit because many of the questions in the RFI were not directly related to provisions in the Registry Agreement (RA), making them outside of the permissible scope of an audit under the terms of the RA. This communication is posted to ICANN's correspondence page.

In that communication, the RySG requested that the out-of-scope questions be removed from the audit and that each audit question reference the specific contractual clause to which it pertains, so all parties can track the origin of each audit inquiry. The RySG reiterated this request during two webinars conducted by Compliance on 5 November 2018.

On 8 November 2018, Jamie Hedlund responded to the RySG's communication. Regarding the request to have "each audit question reference the specific contractual clause to which it pertains," Mr. Hedlund asserted that the questions are designed to be generic in light of the different agreements and noted that Compliance will not amend the RFI to denote each question with the section of the RA to which it corresponds. Instead, the individual, initial and final audit report sent to Registries will tie the findings to the specific obligation.

The RySG does not consider this to be an adequate response. By its own admission, Compliance concedes that some questions in the RFI may not be based on requirements contained in the RA, yet Compliance has declined to make changes to the RFI to better align with ICANN's contractual remit. The undefined and expansive scope of the RFI is not acceptable.

Compliance identifies "transparency through communication" as important to its approach, and transparency more generally is an important tenant codified in ICANN's Bylaws. Yet, Compliance's refusal to map the RFI requests with the applicable RA provisions abrogates the principle of transparency in what we believe to be an unsettling and opaque attempt to grow Compliance's role and scope well beyond what is permissible under the RAs.

RySG Concern

The RySG is filing this Complaint because many of the questions contained in the RFI are out of scope of a permissible audit under the RAs. Specifically, some of the questions included in the RFI:

(1) are outside ICANN's audit rights as set forth in the respective RA;
(2) are not tailored to assess compliance with obligations contained in the RA; and
(3) reflect an expansive view of Compliance's mission.

As a party to the RAs, Registries are keenly aware of the scope of ICANN's audit rights, which are as follows:

> For the new gTLD RA, ICANN may "conduct, contractual compliance audits to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement and its covenants contained in Article 2 of this Agreement." New gTLD RA, Section 2.11.
>
> For legacy TLDs, the scope of audits is limited to "representations and warranties contained in Article II of this Agreement and [Registry Operator's] covenants contained in Article III of this Agreement." Legacy gTLD RA, Section 3.

The above two provisions represent ICANN's scope of audit for gTLD Registries; anything that falls outside of these provisions is necessarily out of scope and not properly subject to audit by ICANN. Further, audits must be "tailored to achieve the purpose of assessing compliance." New gTLD RA, Section 2.11. In other words, the audit cannot be used as a means by which ICANN Org may seek information beyond how Registries comply with the aforementioned contractual provisions.

The RySG recognizes that ICANN Org is trying to leverage its Compliance function to review Registries' Registry DNS abuse monitoring and mitigation processes. As the RySG stated in a comment to Compliance's 8 November 2018 blog, we agree this is a worthwhile and important endeavor. The RySG takes seriously the concerns expressed by members of the community regarding DNS infrastructure abuse and are willing to engage and work constructively with the community and ICANN Org to address and respond to those concerns. Registries have a vested interest in ensuring that we offer a reputable product that consumers can trust, and value prompt action to mitigate DNS abuse - above and beyond the requirements of the RA. ICANN's Compliance department, however, is tasked solely with ensuring that contracted parties are upholding their *contractual* obligations with respect to DNS infrastructure abuse and security threats, not with performing what amounts to a voluntary inquiry under the auspices of an audit of practices that fall outside the RA under the auspices of an audit.

Under the new gTLD RA, the contractual obligation specific to DNS abuse is laid out in Specification 11 3(b) (which is, in turn, incorporated into Article 2 through Section 2.17, and is subject to Compliance's audit right). That provision requires Registries to (1) periodically conduct a technical analysis to assess security threats in the TLD, (2) maintain statistical reports on the number of security threats identified and actions taken, and (3) to provide these reports to ICANN upon request. Registries have routinely provided Compliance with such statistical reports in past audits.

The current RFI seeks information well beyond what is required to assess Registries' compliance with the relevant provisions in the various RAs, asking questions that are not "tailored to achieve

the purpose of assessing compliance" with Specification 11 3(b), and are therefore out of scope of a contractually permissible audit. There are no contractual requirements specific to the form, timing or function of a Registry's "technical analysis" or "actions" - Registries are not obligated to provide information on how we identify security threats, why we do or do not report issues to registrars, share analysis with other parties, or review industry blogs, etc. Seeking this type of information through an audit is an abuse of ICANN's limited right to audit particular contractual provisions and constitutes significant overreach of the Compliance function.

The RySG is concerned that ICANN will view this audit as precedential with regard to Compliance's search for information outside existing reporting requirements, or worse, that the audit indicates ICANN Org's future intentions to work to embed the voluntary Security Framework (which was always intended to be, and is explicitly on its face, a voluntary document) into our Agreements. Registries are bound to honor the requirements of and adhere to the restrictions contained in our RAs. ICANN Org is similarly bound by contractual restrictions and should be held to the same standard.

Suggestion for an Alternative Approach

The RySG has no issue with GDD staff conducting a voluntary survey of contracted parties on DNS abuse monitoring and mitigation, or security practices. Indeed, that would be an appropriate and likely fruitful path to obtain the information sought in this RFI. But to frame these requests as a required contractual audit intentionally ignores the limits put on ICANN Org under the RAs.

Because audit questions, by their very nature, imply an inherent threat of enforcement action, it is not appropriate to use an audit to gather data about Registries' security practices. Moreover, this approach is unproductive for all parties and does little to foster trust between ICANN Org and contracted parties. This is especially true considering the willingness of Registries to engage in an open and forthcoming dialogue on these issues outside of the compliance venue.

Data Privacy Concerns

While the concerns regarding scope are primary to this audit, the RySG has also made clear to Compliance staff the concerns we have regarding how ICANN Org handles personal data received from contracted parties.

Contracted parties have consistently raised concerns regarding the lack of data protection measures governing data transfers to ICANN for Compliance tasks. These concerns were articulated during the ICANN63 RySG session and again during the Compliance audit webinars. To date, ICANN Org's statements in response remain insufficient to address our concerns. Such matters are of high importance to both parties of these contracts and represent risk that should be specifically addressed.

The RySG notes that: (1) continued requests for data transfers to ICANN org without a valid data processing agreement (DPA) in place exposes all parties to liability risks under the GDPR; (2) ICANN has not properly considered Chapter V of the GDPR and no valid basis has been

established for the transfer of data to ICANN Compliance; and (3) the redaction request under the RFI is insufficient to address the data protection concerns related to data transfers.

Understanding that that the community is undertaking a comprehensive review of data protection issues, we anticipate that data processing agreements will be amended; this does not, however, negate the need for a valid DPA between ICANN and contracted parties now.

We recognize Compliance has requested that data to be sent in fulfilment of the RFI in 'redacted' form. Such a request is welcome; however, this is a high level catch all provision that does not define the legal basis and grounds for such disclosure, or address the risk of inadvertent disclosure by ICANN.

In the absence of appropriate safeguards, Registries in our role as data processors within the context of the Compliance audit process, and further to our obligations under Art 28 (3), hereby notify ICANN Org in its role as controller that the RySG remains dissatisfied that the legal requirements for such transfers have been met. We hereby seek cooperation from ICANN Org to further discuss and develop appropriate data protection considerations governing our interactions with Compliance.

Conclusion

Due to the events and issues outlined above, the RySG believes it would be inappropriate for Registries to respond to questions in the RFI that are clearly out of proper scope. The RySG asks that you investigate this matter and provide guidance to ICANN Org that brings this audit, and future audits, within the scope of Compliance's contractual remit, specifically the enumerated Articles contained in the relevant RA (Articles 1 and 2 for the new gTLD RAs and Articles II and III for the legacy RAs).

Supporting Documents

- Copy of RFI Audit Request and Questions: https://www.icann.org/en/system/files/files/contractual-compliance-proforma-dns-infrastructure-abuse-registry-audit-rfi-07nov18-en.pdf
- RySG letter to ICANN Compliance, November 2, 2018: https://www.icann.org/en/system/files/correspondence/austin-to-serad-hedlund-02nov18-en.pdf
- ICANN Contractual Compliance webinars:
    - https://participate.icann.org/p2qjkmr34kp/
    - https://participate.icann.org/p4ajstwsygh/
- ICANN Compliance Response to RySG, November 8, 2018:https://www.icann.org/en/system/files/correspondence/hedlund-to-austin-08nov18-en.pdf

- RySG Comments to ICANN Compliance Blog, November 11, 2018: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse