

**From:** Donna Austin  
**Date:** November 2, 2018  
**To:** Maguy Serad, Jamie Hedlund

**Subject:** Upcoming Registry Audit

Dear Jamie and Maguy,

Thank you for sharing the anticipated audit questionnaire with registries in advance of the formal process. After review, however, the RySG has concerns regarding the breadth of the scope of the proposed audit.

Under the Registry Agreement, audits must be “tailored to achieve the purpose of assessing compliance” with a registry’s reps and warranties. In this instance, Compliance is seeking to determine whether registries comply with Section 2.17 “Additional Public Interest Commitments” as set forth in Specification 11 3(b).

That provision requires registries to (1) periodically conduct a technical analysis to assess security threats in the TLD, and (2) maintain statistical reports on the number of security threats identified and actions taken. Previous audit rounds asked “Does your Registry Operator periodically conduct a technical analysis outlined in Specification 11 3(b)? If you answered ‘yes’ to the above question, please upload a copy of the most recent technical analysis report.” As those questions were sufficiently tailored to assess registry compliance with the same contractual provision for the past 5+ years, it is not clear how ICANN can now justify some of questions contained in this audit RFI.

The RySG is concerned that ICANN is using its contractual right to audit registries as the basis to conduct what should be a voluntary request for information about the practices of registries with respect to their security practices. The RySG has no issue with GDD staff conducting a voluntary survey of registries on their security practices. But to frame this as a required contractual audit, and conducting this through contract compliance, we believe is overstepping the rights afforded to ICANN under the Registry Agreement.

Audit questions from Compliance are accompanied by an implied threat of enforcement action. With the scope of some questions asked in the draft RFI that implied threat of enforcement action is unwarranted as they exceed a Registry Operator’s contractual obligations. Any questions beyond those which are tailored to assess compliance with a specific contractual provision should be specifically identified as optional, noting the reasons & benefits for making each ask.

If ICANN continues to approach this security request for information as an “audit”, registries are required to provide information “reasonably necessary to demonstrate Registry Operator’s compliance.” Given that there are no contractual requirements specific to the form, timing or function of the “technical analysis” or registry “actions” taken, registries are not obligated in an audit to provide Compliance with information explaining how we identify security threats, why we do or do not report issues to registrars, or share analysis with other parties.

In addition to removing the out of scope questions from this audit, we request 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 appreciates that Compliance has scheduled webinars next week and looks forward to walking through each question in the RFI as well as the general scope and nature of the audit with you at that time.

Regards

Donna

Donna Austin  
Chair, Registries Stakeholder Group