RAA NEGOTIATION ISSUES

This memo describes the current procedural state of the RAA negotiations and, more importantly, the key issues that remain open. For a complete briefing on all the issues please see the companion **Summary Chart** listing each of the negotiation topics.

The outstanding issues and the negotiation status give rise to the topics for public discussion in the ICANN Prague meeting. Those issues, including specific sub-issues, are described in the second half of the paper. The session is scheduled for Monday, 25 June 2012. The agenda can still be adjusted. If you have a suggested topic for consideration, please provide comments on the RAA Amendment Negotiations section of the ICANN Community Wiki, at https://community.icann.org/display/RAA/Negotiations+Between+ICANN+and+Registrars+to+Amend+the+Registrar+Accreditation+Agreement.

NEGOTIATION STATUS

Current Situation and Recent Developments

Since the Dakar meeting, ICANN and the Registrars have engaged in 18 extended negotiation sessions to amend the Registrar Accreditation Agreement (RAA). These have been supplemented by information and document exchanges between discussions. The negotiations are progressing on each of the 12 law enforcement and the GNSO recommendations (as well as specific requests by ICANN and the registrars). There are many areas where ICANN and the registrars are in agreement and a few important ones where there are still differences. A **Summary Chart** summarizes key areas of progress is posted with this memo. ICANN thanks the Registrar Negotiating Team for their continued participation in this process; it now appears to be time to bring others within the ICANN community into the conversation to help inform the conclusion of negotiations on a few key areas.

While there are 12 separate law enforcement recommendations (and all are being addressed), we think there are four that rise above the others in importance:
(1) verification / validation[1] of Whois data;
(2) enhanced collection of information related to registrants (data retention);
(3) enhanced obligations regarding resellers and privacy/proxy services; and
(4) creation of contacts for reports of domain name abuse.

There is agreement on the creation of a proxy/privacy accreditation service and operating abuse points of contact. There remain fundamental differences in two important areas: (1) Whois verification and (2) data retention requirements. After requests for clarification, ICANN received law enforcement memoranda on these two issues on 8 May 2012 and 30 April 2012 respectively, and the ICANN negotiating team adopted the law enforcement

[1] Validation refers to checking the format and completeness of the data, verification refers to checking that the contact points work by sending a message or calling,

clarifications as ICANN's negotiating position. We also recognize that community discussion is needed on these complex issues to determine the appropriate balance of meeting the public's interest and matching the goals behind the law enforcement requests. For example, one consideration is the potential costs to registrants and registrars that may be associated with the implementation of the requests. Another is the benefit of accruing from a substantial first step in improving Whois accuracy.

Because these two areas are so important, ICANN and the registrars are not able to post consolidated, negotiated amendments in advance of the Prague meeting. The draft RAA posted reflects ICANN's most recent proposal. While much has been agreed between ICANN and the Registrars, ICANN is providing information on the continued areas of disagreement to inform a community discussion that will help bring these final issues to closure.

Other Amendment Topics

Both ICANN and the registrars are raising additional items beyond the law enforcement and GNSO recommendations for inclusion in negotiation. The registrars have proposed: (1) a new process for amending the RAA; (2) removal of Port 43 Whois obligations for "thick" gTLDs; (3) clarification of the Consensus Policy Development section; and (4) automatic accreditation in all new gTLDs.

ICANN has proposed: (1) improved termination and compliance tools; (2) streamlined arbitration; (3) limitation of time for request of stays for negotiations; and (4) a prohibition against cybersquatting by registrars and their affiliates.

While substantial agreement on proposed terms has been reached on many of these "other" amendment topics, ICANN has continued to note the need for agreement on the key topics of Whois verification and data retention prior to publishing a proposed agreement in these other areas. For example, it is difficult to concede changes to the RAA amendment process (requiring bilateral negotiations) without giving up negotiating leverage on law enforcement proposals on Whois verification and data retention.

AGENDA FOR PUBLIC MEETING

<u>Key Areas for Community Input</u>

Below we provide some key questions and points of information that we hope to guide the community discussions in Prague. We seek a discussion and input from the community as to where ICANN should hold firm to the proposals within the law enforcement recommendations on Whois verification and data retention issues, and where further negotiation might be required. The pros and cons on these and other issues that should be discussed in a public session are provided below. We also seek discussion on how to assure that, when the new RAA is eventually approved, all Registrars will move to the new agreement.

Specific questions and points to help pinpoint the issues are:

Pre-resolution Verification

Law enforcement recommends the verification of registrant Whois data *before* allowing a new domain name registration to resolve. The Registrars are willing to agree to verify registrants within a certain time *after* the resolution (such as 5 days), with a requirement to suspend the registration if verification is not successful in that interim time period.

Registrars state that: (1) currently, domain names resolve immediately upon registration and changing that practice and delaying resolution for a period of days should be a policy discussion as it dramatically changes the domain name registration market; (2) this attempt to stop the tiny percentage of wrongdoers materially inconveniences the legitimate registration of millions of domain names; and (3) registrants often obtain domain names in order to obtain an email address (associated with the new domain name) so verifying the email addresses prior to registration is not feasible.

Law enforcement states that domain names abuses can be effective even if the domain name is held only a few days and so verification prior to allowing the name to resolve is necessary.

- Should the process of registering domain names be changed to perform Whois validation and verification *before* domain names are allowed to resolve?

- Will pre-verification address law enforcement's concern?

- How big of a change is this to the current registration marketplace?

- What are the costs to Registrars in modifying their systems to allow for pre-verification?

- What are the costs to registrants?

- How does the fact that registrants often submit a domain name registration request in order to obtain an email address affect the discussion?

Phone Verification

The law enforcement proposal requires verification of email (requiring the return of a unique code) *AND* phone numbers through processes such as calling the phone or sending a SMS and requiring the return of a unique code. Registrars are willing to verify through one of: (1) an email requiring a return of a unique code; (2) phone number through processes such as calling the phone or sending a SMS; *OR* (3) verification thorough postal mail. The Registrars propose that the choice among the three options would be made by each registrar.

Registrars state that: (1) phone verification will dramatically increase costs for some registrars, putting small registrars out of business; and (2) wrongdoers will easily pass this test. Registrars note that due to the variety of Registrar business models, some Registrars may actually prefer phone verification over email verification at this time, but not all Registrars are equipped to perform phone verification.

- Should registrants be required to have a phone number? (Currently the registrar only has to publish telephone numbers for the administrative and technical contacts, not for the Registered Name Holder.) How else might this impact registrants?
- What are the actual technical and financial burdens for Registrars?
- Will this encourage the use of proxy services? (Proxy services might also be required to verify the contact details of their customers.)
- What goals will phone verification achieve?

Annual Re-verification

The law enforcement proposal requires annual re-verification of registrant information. The Whois Reminder Policy has limited effect on Whois accuracy, and some in the community argue that it should be augmented with annual verification.

The Registrars are willing to maintain responsibility for sending Whois reminder policy notices OR verifying information *when changed* by the registrant. Registrars state that an annual re-verification requirement imposes significant costs without additional benefit.

- How much of a burden would annual verification impose on legitimate registrants, including those registering large numbers of names?
- Is requiring the cancellation of a domain name if the annual re-verification cannot be completed too high a penalty? Are the possible unintended consequences disproportionate?
- What are the actual technical and financial burdens for Registrars?
- What goals will this re-verification achieve?

Data Retention

Law enforcement has requested that all identified data elements be kept for two years past the life of the registration.

The Registrars have raised questions regarding their universal ability to retain the data identified by law enforcement, citing various data privacy laws. Registrars are willing to retain most of the information requested by law enforcement. Registrars state that some elements such as transaction data can only be retained for six months (not six months *after* the expiration of the domain name, just six months). Registrars state that this is due to data privacy laws in certain jurisdictions. The Registrars have expressed concerns that registrars in jurisdictions with less-restrictive data protection/privacy regimes will be put at a disadvantage if they are required to maintain registrant data for the full term requested by law enforcement, which is two years past the life of registration, while registrars in other countries may not be able to keep this information for more than 6 months from creation.

- Is the duration proposed by law enforcement proportionate with their objective, or does it place too high a burden on registrants and Registrars?
- How should ICANN monitor compliance with a two-year plus retention period when many of its accredited Registrars might not be permitted to meet that duration? Is this counter to a goal of uniformity in contracts across Registrars?
- Does the GAC (or do the governments participating through the GAC) agree with the clarifications proffered by law enforcement? Can authorities expert in data privacy assist in proposing how ICANN and the Registrars should address the competing legal regimens into a standard that can be uniformly implemented?
- Are any of these requirements already imposed at a national level?

Universal Adoption of RAA

The Registrar Negotiating Team has requested, and ICANN agrees, that it is essential to consider how to require and/or incentivize universal adoption of this new RAA. The accreditation model is based upon having a uniform contract applicable to all ICANN-accredited Registrars, and those moving to the new RAA will face many new obligations. ICANN and the Registrars have been working hard to create a globally acceptable improved RAA. How can global implementation be best achieved?

Some ideas that have been suggested either in negotiations or publicly by interested parties:

- Begin limitations on the terms of accreditations and renewals under the 2009 RAA to allow all registrars to move to the new RAA together.
- Creating milestones for the phasing in of certain terms under the new RAA, so that more Registrars would be subject to the new RAA when the terms come into effect.
- Providing incentives for adoption of the new RAA prior to the expiration of a Registrar's current RAA.
- Use of a Registrar Code of Conduct process to require certain terms to be followed by all Registrars, regardless of whether they are on the 2009 RAA or the new RAA.

- Requiring use of the new agreement when registering names in new gTLDs.

See the **Summary Chart** for more details on key areas of progress in the RAA negotiations.