Discussion Paper

On Next Steps to Produce a New Form of

Registrar Accreditation Agreement

(including reference documents)

13 October 2011

I.   Executive Summary

This Paper responds to requests arising out the ICANN Board's discussions with the Registrar Stakeholder Group during recent ICANN meetings[1] to facilitate consideration of proposals to amend the Registrar Accreditation Agreement (RAA), to address proposals identified by the Joint GNSO/ALAC RAA Drafting Team[2], and representatives from the law enforcement community.[3] Recognizing that efforts have been recently initiated by the Registrar Stakeholder Group to address some of these law enforcement issues (including, a request for an Issue Report which was approved by the GNSO Council),[4] and the GNSO Council is to vote on a motion regarding next steps for the RAA (referred to as the "Modified Process B"),[5] this Paper identifies alternative paths for considering the broader list of amendment topics.

ICANN was specifically asked to classify recommended changes to the RAA as being inside or outside the "picket fence," that is, whether each of the topics could be the subject of a new Consensus Policy binding on registrars.   Undertaking that analysis and engaging in discussion with multiple stakeholders has resulted in the following recommendations and conclusions that are explained in this Paper:

1.   It is nearly impossible to classify "topics" as suitable for policy discussion. As described below, all topics are classified as available for GNSO policy discussion but whether the resulting recommendations lie inside or outside the "picket fence" depends on the details and the path taken.
2.   Registrars and ICANN should start negotiating RAA amendments immediately. The negotiations would be bi-lateral with extensive, detailed, timely reporting to the community to ensure transparency. This is in-line, we think, with the

---

[1] See, for example, the Singapore transcript posted at: http://singapore41.icann.org/meetings/singapore2011/transcript-board-registrar-21jun11-en.pdf.
[2] See the proposed amendment topics from the RAA Final Report, as described on Annex 1- High Priority Topics, and Annex 2- Medium Priority Topics.
[3] See the proposed Code of Conduct developed by representatives of the law enforcement community, as described on Annex 3
[4] See the Registrar Stakeholder Group Law Enforcement Communication included in Annex 4, which describes these efforts, and the amended motion originated by Tim Ruiz on behalf of the Registrar Stakeholder group, which was passed at the GNSO Council's 6 October 2011 meeting.
[5] See motion by Kristina Rosette, posted at: http://gnso.icann.org/mailing-lists/archives/council/msg12083.html, as described on Annex 5.

latest proposals to the GNSO Council. The first session would focus on the reporting process (including a timeline) for the discussions so that the transparency plans can be reported to the community.

3. While this Paper does not make a specific recommendation about the process for approving the amendments, we think progress on substantive issues will lead to resolution on process. As described below, there are multiple ways to producing a new form of RAA, some which are more expedient then others.

4. We also note that disagreements in the GNSO Council regarding the process over the last year have resulted in delays in considering the substantive issues. Attempting to make progress on these substantive issues immediately may produce tangible results in a shorter timeframe than suggested in the Modified Process B Motion pending before the GNSO Council.   In any event, the GNSO Council would still play an important role in approving the form of the new RAA that results from either this Staff Proposal or the Modified Process B.

5. This Paper or its conclusions are not intended to in any way forestall consideration of the issues in front of the GNSO, such as the request for an Issue Report with regard to specific discussion of law enforcement recommendations.

6. It is our conclusion that the GNSO can take up any of the amendment topics at any time as a policy matter. These recommendations are meant to be considered *in parallel* with any policy discussions that the GNSO may consider with regard to any of the amendment topics.   As stated above, the specifics of those discussions will determine whether they are a "policy" matter.

7. Registrars and Law Enforcement representatives are encouraged to continue their dialogue. Law Enforcement goals are important to ICANN and work toward the benefit of Internet users; Registrars bring unique knowledge as to the workings of the DNS and how the Law Enforcement objectives can be achieved. Progress and understanding, though, will require intensive, detail-oriented work. It is suggested that a process for working through these topics could be identified during the Law Enforcement session on Monday during the Dakar meeting.

This Paper describes the different options available for producing a new form of RAA, and provides a possible alternative option, which consists of a multi-tier approach that adopts one approach for those topics which might be more quickly negotiated with the Registrars, accompanied by what might be a longer-term approach for those topics that could be evaluated through a GNSO Council policy development process (PDP). These longer-term options may result in a new consensus policy, or a new form of RAA.   Section V below identifies which of the proposed amendment topics may be appropriate for consideration under a PDP, or under other available processes.

II.   Objective

This Paper is published in advance of the Dakar ICANN Meeting in support of the important efforts underway to improve the RAA. As a party to the RAA, ICANN is responsible for enforcing its terms, and desires to facilitate further dialogue to support focused policy development efforts and encourage the adoption of an amended version of the RAA.

The analysis described below is intended to highlight the options available for policy development and to produce a new form of RAA.   The objective of this effort is to provide a starting point that can establish some common ground to facilitate these discussions, and to provide suggestions for a process to adopt an amended RAA in a collaborative and timely fashion.

III.   Background

The Registrar Accreditation Agreement (RAA) was last amended by the ICANN Board in May, 2009.   At the time, the proposed 2009 RAA was controversial, with some community members supporting it and others insisting that it had not gone far enough to address concerns.[6]

The GNSO Council's unanimous recommendation to the ICANN Board to approve the 2009 RAA was tied to an agreement to continue work on identifying additional amendments to the RAA. This led to the formation of a joint drafting team ("RAA-DT") with members of the GNSO and At-Large Community to come up with proposals to improve the RAA. The RAA-DT's Final Report on Proposals for Improvements to the Registrar Accreditation Agreement (RAA Final Report) included a list of specific topics for potential future amendments to the RAA, as well as a proposal for next steps for the GNSO Council to consider in producing a new form of RAA.

After review of the RAA Final Report, the GNSO Council was unable to reach a consensus on a process to move the RAA improvements forward, reflecting the differences within the community on both substantive and process issues.[7]   To date, the GNSO Council has not undertaken any further work to advance the recommendations contained in the RAA Final Report pertaining to amendments to the RAA.[8]

Separately, over the past two years the law enforcement community and Registrars have held several meetings to discuss law enforcement proposals to address their concerns with e-crimes and DNS abuse. The content of the discussions was based on LE proposals for RAA amendments (some of which were included among the topics in the RAA Final Report), such as enhanced due

---

[6] See the minutes of the GNSO Council's meeting on 9 Jan 2009 posted at: http://gnso.icann.org/meetings/minutes-gnso-08jan09.html.

[7] These differences relate primarily to whether any amendments to the RAA should be developed through a PDP process and/or direct negotiations between the Registrar Stakeholders Group and ICANN staff only; whether any additional parties should be allowed to participate and/or observe; and which topics for potential amendments are more appropriate for policy development as "new policies" rather than changes through the RAA.

[8] Although no further work has been done on the RAA Final Report (except for approving the form of the Registrant Rights Charter), the GNSO Council is considering a motion submitted by Kristina Rosette that, if passed, may initiate such work.   See: http://gnso.icann.org/mailing-lists/archives/council/msg12083.html. The motion submitted by Tim Ruiz, passed by the GNSO Council at its meeting on 6 October 2011 may lead to the initiation of a PDP on certain of the law enforcement recommendations, after the GNSO Council considers the Issue Report requested of Staff.

diligence on Registrars, and a proposed Registrar Code of Conduct.[9] These LE recommendations were endorsed by the GAC in Brussels, and were subsequently highlighted in various GAC communiqués.[10] Apart from the GAC-LE discussions, these proposals were discussed separately between LE and Registrars for practicality. Registrars responded to those discussions in writing, and from that and subsequent discussion, it is clear that additional dialogue is necessary to develop a mutual understanding regarding the best way to implement amendments and combat abuses. These independent meetings were aimed at encouraging Registrar-LE dialogue, evaluating LE proposals, and producing a voluntary cooperation model outside of ICANN's processes and policies. More details on the substance of the proposals evaluated can be found in the Registrar Stakeholder Group Statement attached as Annex 4, and the Code of Conduct, attached as Annex 3 proposed by the LE representatives, which was discussed in Singapore,[11] and referenced in the GAC Singapore Communiqué.

Staff understands that although these independent efforts to produce a voluntary LE/registrar cooperation model have not yet resulted in substantive change, a GNSO Council motion was submitted by Tim Ruiz [12] on behalf of the Registrar Stakeholder Group to address some of the law enforcement recommendations through a new policy development process (PDP). Registrars have made clear to ICANN staff their intention to continue cooperating with LE to address the policy and amendment requests as embodied in the remaining law enforcement recommendations or the RAA Final Report recommendations. The GNSO Council voted to request an Issue Report as requested by the Registrar Stakeholder Group on certain law enforcement recommendations at its meeting on 6 October 2011.

      This Discussion Paper is published to summarize options for processes by which the amendment topics that are generally acceptable to Registrars can be implemented in a timely manner, as well as the more formal processes for those topics that either need further evaluation and analysis, or reflect new policy positions.

---

[9] The LE proposals were attached to the Final Report on Proposals for Improvements to the Registrar Accreditation Agreement in Annex G.

[10] https://gacweb.icann.org/download/attachments/1540134/Singapore+Communique+-+23+June+2011_2.pdf?version=1&modificationDate=1312392506000

[11] A transcript of the meeting between the GAC and the Registrar Stakeholder Group in Singapore, where the Registrars shared their concerns regarding the proposed code of conduct is posted at: https://gacweb.icann.org/download/attachments/1540134/gac-gnso-registrar-21jun11-en.doc?version=1&modificationDate=1312468013000

[12] See motion by Tim Ruiz, posted at: https://community.icann.org/display/gnsocouncilmeetings/Motions+22+September+2011.

IV. Several Options Available to Produce a New Form of RAA

There are several ways to produce a new form of RAA, as described below. One path that the parties to the contract, the GNSO Council and others might find desirable would be a staged plan of action, where the broadly acceptable topics could be identified, negotiated and adopted through one process, and the more complex topics could be evaluated and adopted through a longer term process.

A. Contract-Based Options

- **2009 RAA Process.** In 2009, following two years of negotiations, ICANN and members of the Registrar Constituency arrived at a set of amendments for inclusion in the new form of RAA. At the same time, two public comment forums were opened in an effort to solicit input from the community on the new proposed form of RAA. Following this public comment forum, the GNSO unanimously recommended adoption of the 2009 RAA, and the Board adopted it, thereby making it the mandatory form of RAA for all new and renewing registrars.[13]
- **Additional Requirements for New gTLDs.** It may be possible to incorporate additional commitments through the inclusion of new terms in the Appendices to the RAA to be used by ICANN to authorize a registrar to be accredited for the New gTLD Program.   Currently, registrars sign a new appendix for each TLD for which they are accredited.[14] This "New gTLD Appendix" could include the recommended amendment topics that are identified as generally acceptable to the registrars from the LE recommendations and/or the RAA Final Report.   To achieve this, ICANN could commence a series of consultations with the community, and engage in negotiations with the registrars and discussions with law enforcement representatives to produce the new terms, which could then be posted for public comment. The development of this New gTLD Appendix could be done in a manner that would not affect the timing of the launch of the new gTLD Program, as it could occur in parallel with the applications being received and evaluated.

---

[13] These efforts were coupled with an incentive program designed to encourage the early adoption by registrars of the new 2009 RAA. This approach was successful, leading to adoption by a substantial number of registrars of the 2009 Agreement.

[14] See the current appendices used by ICANN, as posted at http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm

- **Advisory for Clarifications of Existing Obligations.** Some topics might be addressed by clarifications of existing obligations under the RAA, which could be dealt with through the form of an ICANN advisory to be developed in consultation with the Registrar Stakeholder Group, and published for public comment.

- **Code of Conduct.** Several topics could be dealt with through a Code of Conduct, rather than inclusion in the RAA, in order to expedite adoption among Registrars.   The RAA Section 3.7.1 states:

    "In the event ICANN adopts a specification or policy, supported by a consensus of ICANN-Accredited registrars, establishing or approving a Code of Conduct for ICANN-Accredited registrars, Registrar shall abide by that Code."

    Several topics may be ripe for consideration for inclusion in a Code of Conduct as referenced in the RAA.   These items could include those where it is likely that a consensus could emerge from the Registrar Stakeholder Group.

B. Policy Development Options[15]

- **PDP on New Policy Initiatives.** Some of the topics reflected in the Final Report and in the LE proposed Code of Conduct reflect new policy initiatives that should be explored through formal PDP processes.   Initiatives to introduce entirely new obligations, such as the creation of an ICANN accreditation process for proxy/privacy services, or which introduce verification requirements, are examples of significant undertakings (that would include development and expense) that could be more appropriately addressed through a PDP on the specific topic. A Policy Development Process would follow the process outlined in Annex A of the ICANN Bylaws.[16]

- **PDP on Contractual Conditions for the RAA.** Other topics may be less controversial, and could be combined into a single PDP on "Contractual Conditions for the Registrar Accreditation Agreement," similar to that which was done in 2006, when the GNSO Council commenced a PDP on the issues relating to ICANN's gTLD registry agreements.[17]   That effort led to a GNSO

---

[15] These long term options would likely take 1-2 years, based upon past experience and work-load of the GNSO Council.

[16] Annex A, which describes the procedures applicable to PDPs is posted at: http://www.icann.org/en/general/bylaws.htm#AnnexA.

[17] For more information on the Feb06 PDP, please refer to: http://gnso.icann.org/issues/gtld-policies/council-report-to-board-PDP-feb-06-04oct07.pdf.

recommendation that was adopted by the ICANN Board in 2008.[18] Many of the topics identified below could also be included in a PDP on Contractual Conditions for the RAA.

V.   CATEGORIZATION OF SPECIFIC AMENDMENT TOPICS

This Section responds to requests made at recent ICANN meetings[19] during the Board's discussions with the Registrar Stakeholder Group with regard to the RAA.   Specifically, this section addresses inquiries regarding whether specific amendment topics are "within the picket fence."[20]   This Section also would be responsive to Step 1 of Modified Process B.

Under the Bylaws, the GNSO is responsible for developing and recommending to the Board substantive policies relating to gTLDs. This mandate is by nature broader than what may constitute "consensus policies."   It is important to understand that the GNSO may initiate a Policy Development Process (PDP) on a topic that is within the GNSO Council's mandate, even if it might not ultimately result in a new "consensus policy" that is "within the picket fence."   For example, the GNSO can conduct a PDP on topics related to gTLDs that may result in other types of recommendations, such as advice to the ICANN Board, creation of best practices, or other non-binding policies.

A topic is generally considered to be "within the picket fence" if it falls into subjects recognized under the RAA[21] that, if recommended by the GNSO Council (with the appropriate voting thresholds) and approved by the ICANN Board, could become "consensus policies" binding upon all registrars.   The RAA describes a series of topics where consensus policies could be developed.

---

[18] For more information on the Board's adoption of the GNSO recommendation in this regard, please see: https://community.icann.org/display/tap/2008-01-23+-+GNSO+Recommendation+on+Contractual+Conditions+for+Existing+**gTLD**s+%28PDP-Feb06%29.

[19] See, for example, the Singapore transcript posted at: http://singapore41.icann.org/meetings/singapore2011/transcript-board-registrar-21jun11-en.pdf.

[20] For a more in-depth explanation of consensus policies, please see the presentation from the Sydney ICANN meeting at: http://gnso.icann.org/correspondence/scope-consensus-policy-01jun09.pdf.

[21] See, for example, RAA Section 4.2- Topics for New and Revised Specifications and Policies, posted at: http://www.icann.org/en/registrars/agreements.html.

The chart included on Annex 6 identifies the "High Priority" and "Medium Priority" items, as designated by the RAA-DT, as well as the topics from the LE proposed Code of Conduct, and highlights whether certain of the processes described above in Section IV might be applicable.

Annex 6 does not, however, attempt to categorize these topics as "within the picket fence" because more specificity is required in order to make this determination. That degree of specificity is not attained until amendment details are discussed. Thus, even though it is highly desirable to do so, it is not meaningful to classify a recommendation as suitable for a certain type of policy consideration or inside or outside the picket fence at this point. Typically, this analysis is conducted at a point in the PDP process where the recommendation has developed into a detailed proposal, such as after a working group or negotiating team has published its amendment or policy proposal and submitted it for public comment. Note that in Annex 6, all topics are potential candidates for a Policy Development Process. This, of course, depends on the specifics of the discussion – at the end, some aspects might be "within the picket fence" while certain aspects of the same topic might be outside it.

A few examples might help illustrate the difficulty of making this determination. An amendment topic requiring registrars to accept credit card payments for domain name registrations in order to require registrars to become PCI compliant would likely be outside the picket fence. On the other hand, a requirement that registrars that accept credit card payments must be PCI compliant might be within the picket fence, as it could relate to enhanced verification requirements. Similarly, the new PEDNR policy requiring registrants to receive certain information on renewals was within the picket fence, but if it was accompanied by a requirement that registrars shall not charge more than $100 for renewals of a domain name, this additional requirement would likely be outside of the picket fence.

Because there is more than one path to achieve RAA revisions or new policy applying to registrars, Staff invites the Registrars, and the representatives from the Law Enforcement community, and the ICANN community, to collaborate to identify which processes may be preferable and most effective, to bring about amendments to the RAA.

VI.   Conclusion and Next Steps

Recent efforts made by the Registrar Stakeholder Group to address some of the law enforcement recommendations, as well as the two specific motions submitted to the GNSO Council, are encouraging and constructive in continuing substantive discussions to amend the RAA.   Although Staff will provide resources and support for the Issue Report proposed by Tim Ruiz as approved by the Council, or the Modified Process B should it be approved by the GNSO Council, the following Staff proposal could serve as a possible alternative process for the GNSO Council's consideration:

1. Registrars and ICANN start negotiations on the RAA amendments immediately. The negotiations would be bi-lateral with extensive, detailed, timely reporting to the community to ensure transparency. The first session would focus on the reporting process (including a timeline) for the discussions so that the transparency plans can be reported to the community.
2. Rather than decide the entire process now, we think progress on substantive issues will lead to resolution on process. In the event the process is not clarified during these negotiations, the GNSO Council could then weigh in on the process it recommends to conclude this effort.
3. A new form RAA resulting from this process would be presented to the GNSO Council for its review and, if appropriate, recommendation to the ICANN Board for adoption.
4. Separately, Registrars and Law Enforcement representatives are encouraged to continue their dialogue. Staff suggests that a process for working through these topics could be identified during the Law Enforcement session on Monday in the Dakar meeting.

This alternative is suggested as a means of producing amendments to the RAA in a more time-efficient manner, recognizing the subsequent step of adoption by individual registrars voluntarily or upon renewal.[22] It is important to understand that this alternative has not been vetted with either the Registrar Stakeholder Group, the representatives of the law enforcement community, or the broader ICANN community.   We hope this encourages further dialogue with the GNSO Council and the ICANN community with respect to identifying an acceptable path forward to address the RAA.

---

[22] To encourage early adoption, ICANN could consider offering incentives for early adoption of the new form of RAA, as was done in 2009.

Annex 1- List of High Priority Topics From the RAA Final Report

Item No.	Description	Cross-reference (RAA matrix)	Comments
1	Prohibition on registrar cybersquatting	1.1 through 1.5; comment summary section VI(N)	May include accelerated termination
2	Malicious conduct – registrar duty to investigate	3.1 – 3.3; 3.6	"Duty of registrars to investigate and report to ICANN on actions taken in response to report received from credible third party demonstrating illegal malicious conduct involving DN"
3	Designation and publication of technically competent point of contact on malicious conduct issues, available on 24/7 basis	3.4; 3.5; 5.4	Requirement for registrars; possible requirement for resellers and proxy-privacy services
4	Registrar disclosure of privacy/proxy services made available in connection with registration; and responsibility of registrar for compliance by such services	5.2	Could also apply to such service made available by resellers. Includes, but not limited to, alter ego services
5	Obligations of privacy/proxy services made available in connection with registration re data escrow; Relay function; Reveal function	5.1; 5.3; 5.5; 5.6; 5.7; 5.10	See following item for privacy/proxy services not made available in connection with registration
6	Registrar responsibility for cancellation under appropriate circumstances of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal	5.8; 5.10	This applies to proxy services not offered by the registrar in connection with registration, i.e., independent services. This is where Relay or Reveal function requirements for these services could be spelled out

Item No.	Description	Cross-reference (RAA matrix)	Comments
7	Define circumstances under which registrar is required to cancel registration for false Whois data and set reasonable time limits for registrar action	6.1; 6.6; comment summary section VI(G)	Currently, registrar may cancel, but is not required to do so
8.	Require PCI compliance in registration process	6.9	Or similar pre-existing standard that would assist in verification of registrants
9	Define "reseller" and clarify registrar responsibility for reseller compliance	7.0; 7.1	
10	Require greater disclosure of registrar affiliates/multiple accreditations	9.1; 9.2	Could also apply to "major" resellers (if defined)
11	Require greater disclosure of registrar contact information, information on form of business organization, officers, etc.	9.3; 9.4; comment summary section VI(I)	Information to be verified and stamped with date of last verification
12	Clarification of registrar responsibilities in connection with UDRP proceedings	15.3	Focus is on timelines for registrar response both at beginning and at end of process

Annex 2- List of Medium Priority Topics from the RAA Final Report

1. Spell out "verification" process registrars are required to undertake after receiving report of false Whois data (Matrix item 6.1)

2. Require links to Whois Data Problem Reporting System on Whois results pages and on registrar home page (Matrix items 6.2, 6.3)

3. Service Level Agreement on Whois availability (Matrix item 6.7)

4. Registrar to disclose resellers and vice versa (Matrix items 7.2, 7.3)

5. Expand scope of authority to terminate accreditation (Matrix items 8.1-8.4)

6. Require registrars to report data breaches (Matrix item 10.3)

7. Streamline arbitration process in cases of dis-accreditation (Matrix item 12.1-12.4)

8. Streamline process of adding new gTLDs to accreditation (Matrix items 13.1-13.2)

9. Registrar responsibilities for acts of affiliates (Matrix item 14.1)

10. Staff to draft registrar code of conduct if registrars fail to do so by time certain (Matrix item 17.1)

ANNEX 3- Law Enforcement Proposal Regarding Code of Conduct

At the Singapore Meeting, representatives from the law enforcement community discussed the proposed form Code of Conduct, copied below.

A transcript of the meeting between the GAC and the Registrar Stakeholder Group in Singapore, where the Registrars shared their concerns regarding this proposed code of conduct is posted at:

https://gacweb.icann.org/download/attachments/1540134/gac-gnso-registrar-21jun11-en.doc?version=1&modificationDate=1312468013000

Registrar Code of Conduct
To Enhance Law Enforcement Investigations

INTRODUCTION

This Code specifies the <u>minimum</u> levels of performance by an ICANN accredited registrar for cooperating with law enforcement investigations involving domain names implicated in illegal, criminal, or malicious activities.

I.   COMMITMENT TO COOPERATE [Basis—2.8 of form New gTLD Registry Agreement]

Registrar agree to take reasonable steps to investigate and respond to any reports (including reports from law enforcement and governmental and quasi-governmental agencies) of illegal, criminal or malicious conduct in connection with the use of domain names.

II.   STANDARDS

1.   Use of Proxy or Privacy Registrations

a.   In the event ICANN establishes an accreditation program for proxy or privacy registration services, Registrar will accept proxy/privacy domain name registrations ONLY from ICANN accredited Proxy Registration Services.   Registrar shall cooperate with ICANN to establish an ICANN accreditation program for proxy or privacy registrations.

b.   Registrar will ensure authentic WHOIS information is immediately published when a registrant is found to be violating terms of service, including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity, subject to any applicable cure periods.

2. Prohibition of Certain Illegal, Criminal or Malicious Conduct {Based on Section 5.3.2.1}.

Registrar shall not engage in activities or conduct that results in: (i) a conviction by a court of competent jurisdiction of a felony or other serious offense related to financial activities; (ii) a judgment by a court of competent jurisdiction that Registrar has committed fraud or breach of fiduciary duty; (iii) the Registrar being the subject of a judicial determination that is the substantive equivalent of those offenses (i)-(ii); or (iv) the Registrar knowingly and/or through gross negligence, permitting criminal activity in the registration of domain names or in the provision of domain name WHOIS information, after failing to promptly cure such activity after notice thereof.]

3. Valid Physical Address to be Published.

Registrar must provide a valid physical address for legal service, including a valid street address, city, and region, as well as a valid telephone number and fax number to ICANN.   Additionally, Registrar agrees that accurate and verifiable contact details of (a) the main operational and physical office location, including country, (b) phone number (with international prefix), and (c) street address, city, and region, will be publicly disclosed in the ICANN web directory, as well as posted clearly on the Registrar's main website.   Additionally, Registrar will notify ICANN immediately of any changes to items (a), (b) and/or (c), and concurrently update Registrar's website. Lastly, Registrar will submit URL and location of Port 43 WHOIS server.

4. Valid Officer Data to be Published.

Registrar will display on the Registrar's main website, and update as necessary, the name of the company's executive management personnel, including its CEO and President as well as any other responsible officer(s) or executive(s). The Registrar may include other contact data as appropriate, such as for the legal department or customer service department, to assist in the resolution of issues. Additionally, Registrar will immediately notify ICANN and concurrently update Registrar website of any changes in executive management structure, as well as any changes in the controlling ownership of Registrar.

5. Disclosure of Registrars owned by Affiliates.

Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests.]

6. Notice to ICANN of Certain Changes.

Registrar will notify ICANN immediately of the following:

  a.   Any and all changes to a Registrar's location(s), office(s);
  b.   Changes to presiding officer(s);
  c.   Change in controlling ownership;
  d.   Any criminal convictions, and any civil convictions causal or related to criminal activity.

Registrar will concurrently update their website upon notifying ICANN of (a) –(c) above.

7. Maintenance of Business Licenses.

Registrar will maintain throughout the term of its accreditation with ICANN, and provide to ICANN verifiable documentation that its company is a legal entity within its country of operation, and will provide current, valid, and official certification of business registration(s) or license(s) upon request by ICANN.

8. Publication of Abuse Point of Contacts.

Registrar will prominently publish abuse contact information on their website and WHOIS. The abuse contact will be prominently displayed on its webpage, and a uniform naming convention will be utilized to facilitate discovery of the webpage. The abuse contact information will provide the community with an individual's point of contact information, including telephone and email address. The abuse contact will be an individual who can promptly (within 24 hours) take action to remedy the situation in response to a well-founded report of illegal, criminal, or malicious activity involving a domain name registration.

9. Service Level Agreement for Port 43 WHOIS Access.

Registrar will meet or exceed the requirements of a service level agreement (SLA) announced by ICANN with regards to access to WHOIS information published through Port 43, that addresses the following features: (i) minimum uptime levels for WHOIS servers, (ii) acceptable query limitations and/or IP blocking restrictions, and (ii) minimum data updates frequency.   Registrar will monitor compliance of the ICANN SLA requirements on a monthly basis, and will correct any violations of the WHOIS SLA identified by Registrar or by others within thirty (30) days of

notice thereof.   Failure to satisfy the WHOIS SLA during two consecutive months during any 12 month period may result in notice of SLA violation posted on ICANN's website, or other appropriate ICANN compliance action under the RAA. Registrar shall cooperate with ICANN, as requested, to develop the parameters to be included in the WHOIS SLA.

IV. FURTHER ASSURANCES

The Registrar Stakeholder Group will actively support and encourage the adoption of this Code of Conduct among its membership.   Registrar agrees to support and work with ICANN to include this Code of Conduct into the ICANN Code of Conduct referenced in the Registrar Accreditation Agreement (Section 3.7.1), and to amend the Registrar Accreditation Agreement as appropriate to include the standards referenced herein.   The form of this Code of Conduct may be modified or updated from time to time by the Registrar Stakeholder Group based upon negotiations with representatives of the law enforcement community and/or ICANN.

By signing below, Registrar (and its affiliated registrars) agree(s) to implement and adhere to each of the standards and other terms described in this Code of Conduct.

Registrar Name: _____

By_____
Name_____
Title_____
Date_____

ANNEX 4- Registrar Stakeholder Group Law Enforcement Communication

Communication from Registrar Stakeholder Group

Summary of Law Enforcement – Registrar – Registry Meeting

Brussels, Belgium
24-25 February 2011

From

ICANN Registrar Stakeholder Group

FINAL OFFICIAL COMMUNICATION AS PUBLISHED 17 MARCH 2011

Introduction

In recent years, representatives of international law enforcement agencies (LEAs) have become active in the ICANN community, participating in discussions about combating improprieties facilitated in part through the domain name system (DNS). As a result of those discussions, LEAs have made proposals for policies and/or amendments to contracted party agreements they believed would assist them in more efficiently addressing improper activity.

The Registrar Stakeholder Groups (RrSG) proactively opened a dialog with LEAs to learn more about how the DNS is used for criminal activity, and to inform LEAs about operational and legal considerations relating to LEA proposals. This dialogue began in earnest during the 38th ICANN meeting in Brussels in June 2010, and was followed by a meeting in Washington, DC in September 2010.

While contracted parties and LEAs agreed that the Washington meeting was informative and productive, additional discussion was needed to consider regulatory and legal obligations of contracted parties in Europe and the Asia-Pacific region, as they sometimes conflict with those of US-based operators.

LEAs and contracted parties thus met in Brussels to continue discussions. Generously hosted by the European Commission, the meeting included international LEAs, contracted parties, government officials, and representatives from European and American Regional Internet Registries (RIPE NCC and ARIN).

Summary

The Brussels meeting agenda included:
- Review of LEA recommendations on due diligence in accrediting registrars
- Review of registrar standard operating procedures
- Case examples from EU law enforcement agencies
- Presentations regarding online crime from representatives of ccTLDs, including .gg, .na, .be and .uk.
- A review of the Internet landscape following the introduction of new gTLDs
- A discussion of the recent voluntary collaborative model used to address the sale of illegal pharmaceuticals over the internet (includes registries, registrars, payment providers, shipping companies, search providers, law enforcement, and the US government)

Statements of agreement by meeting participants

<u>Crime and improper activity under the DNS are significant and growing problems that continue to evolve rapidly</u>
Regrettably, crime facilitated through the DNS is a serious issue, and criminal activity develops and changes very quickly. Addressing and reducing criminal behavior demands collaboration and flexibility from a variety of different segments of the Internet ecosystem.

<u>Collaboration to address online crime must focus on objectives and the most practical method to achieve them</u>
While there have been specific proposals—namely, proposed amendments to the Registrar Accreditation Agreement (RAA)—the parties agreed that proposed collaboration should be focused on steps that would be most effective and rapidly deployed, whether or not this included new policy or amending contracts.

<u>Contracts may or may not be the most practical or efficient method</u>
Parties agreed that contracts between ICANN and contracted parties are not policy tools, but at times may represent an effective method for registrars and registries to assist LEAs in their efforts. It is important to consider that amendments to contracts may not be immediately effective (depending on the term of the agreement), so there likely are alternative methods to reach objectives that can have impact sooner.

<u>Consider the entire Internet ecosystem</u>
As cybercriminal activity evolves, the community should consider the entire Internet ecosystem in addressing crime to find the most effective path to solutions. This includes ICANN and its contracted parties, but also ISPs, hosting providers, search engines, payment processors, shipping firms, and others.

<u>ICANN should add more rigorous due diligence to of its accreditation process</u>
Additional diligence in evaluating applicants for registrar accreditation, at minimum, is a good practice and may offer assistance in evaluating who is well suited to provide domain name services and collaborate in online crime prevention.

<u>ICANN must maintain a robust compliance program</u>
For contractual and policy matters that are binding to contracted parties or others, ICANN must consistently and effectively enforce compliance with the terms of their agreements, and terminate accreditations, where appropriate.

<u>Policy or contract amendment proposals must responsibly consider resource and financial costs of implementation, and how costs will be borne</u>
Without considering the burden of implementation, proposed policies will needlessly be slowed by affected parties questioning how costs will be borne and by whom.

Review of LEA proposals

To organize specific discussions about how contracted parties and LEAs can collaborate toward addressing online offenses, participants examined LEAs' proposed RAA amendments. Each issue was thoroughly reviewed to identify the objective of the proposed amendment, hoped-for outcomes, and available paths toward the objectives.

Following is a list of the proposals, noting that further discussion and revisions are needed:

Proposal No. 1
1) The RAA should not explicitly condone or encourage the use of Proxy Registrations or Privacy Services, as it appears in paragraphs 3.4.1 and 3.12.4. This goes directly against the Joint Project Agreement (JPA) ICANN signed with the United States Department of Commerce on September 25, 2006 which specifically states "*ICANN shall continue to enforce existing (Whois) policy*", i.e., totally open and public WHOIS, and the September 30, 2009, Affirmation of Commitments, paragraph 9.3.1 which states "*ICANN implement measures to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information.*" Lastly, proxy and privacy registrations contravene the 2007 GAC Principles on WHOIS.

If there are proxy and/or privacy domain name registrations, the following is recommended concerning their use:

   a. Registrars are to accept proxy/privacy registrations only from ICANN accredited Proxy Registration Services;
   b. Registrants using privacy/proxy registration services will have authentic WHOIS information immediately published by the Registrar when registrant is found to be violating terms of service, including but not limited to the use of false data, fraudulent use, spamming and/or criminal activity.

Summary of Discussion
There was agreement that accreditation of privacy/proxy services has value to consumers. The issue needs further research and discussion in order to understand how ICANN (particularly ICANN staff) would define accreditation parameters, pursue accreditation, educate the community, and seek to accredit current providers of such services.

Proposal No. 2
2) To RAA paragraph 5.3.2.1, language should be added to the effect "or knowingly and/or through gross negligence permit criminal activity in the registration of domain names or provision of domain name WHOIS information..."

Summary of Discussion
There is agreement that language be added to provide notice of the illegal behaviour to the registrar and an opportunity to cure by the registrar would be necessary. Also, paragraph 5.3.2.1 of the RAA may not be the appropriate place for this amendment.

Proposal No. 3
3) All Accredited Registrars must submit to ICANN accurate and verifiable contact details of their main operational and physical office location, including country, phone number (with international prefix), street address, city, and region, to be publicly disclosed in ICANN web directory. Address must also be posted clearly on the Registrar's main website. Post Office boxes, incorporation addresses, mail-drop, and mail-forwarding locations will not

be acceptable. In addition, Registrar must submit URL and location of Port 43 WHOIS server.

Summary of Discussion
Again, there was general agreement that this amendment is not objectionable. At least two alternatives are possible:
- Make the amendment more directly stated: "Registrars must provide a valid physical address for legal service, as well as a valid phone number."
- Amend section 3.16 of the 2009 RAA to specify that a physical address must be provided.

Proposal No. 4
4) Registrars must publicly display of the name of CEO, President, and/or other responsible officer(s).

Summary of Discussion
There was no objection to this, though the amendment needs to be more carefully worded, as the operational reality is that legal issues are often referred to others in an organization.

Proposal No. 5
5) Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests.

Summary of Discussion
For the purpose of eradicating illegal online behavior, there was little certainty that corporate ladder information would provide data necessary to do so.

Proposal No. 6
6) Registrar must notify ICANN immediately of the following and concurrently update Registrar website:

   a. any and all changes to a Registrar's location;
   b. changes to presiding officer(s);
   c. bankruptcy filing;
   d. change of ownership;
   e. criminal convictions;
   f. legal/civil actions

Summary of Discussion

   a. This is agreeable.
   b. This is agreeable.
   c. There was general agreement that this would be difficult and is an unreasonable ask, as it is asking registrars to, in effect, dissuade their own customers' confidence in their stability.
   d. Should be amended to "change in controlling ownership." Note, however, that this may be duplicative since a notifcation to ICANN of a change in "Controlling Interest" is required in the 2009 RAA under section 5.9.2
   e. Perhaps corporate criminal convictions could be reported to ICANN, but publishing such data on registrar websites is not reasonable and may violate privacy laws. Furthermore, official findings by non-criminal regulatory bodies could be reported, to ICANN, as well.
   f. This is impractical, as most civil actions have little to do with combating online crime.

An ICANN board member was present and indicated that ICANN would not, at present, have the operational capacity to collect and manage this data. This proposed amendment would need more discussion.

Generally, the requirement to publish points c) to f) on the registrar website was seen as unnecessarily harmful to the registrar business without positively impacting the cybercrime issues, while a) and b) were seen as redundant with the current RAA.

Proposal No. 7
7) Registrar should be legal entity within the country of operation, and should provide ICANN with official certification of business registration or license.

Summary of Discussion
This is redundant, as ICANN requires this during the accreditation process.

Proposal No. 8
8) Resellers must be held completely accountable to ALL provisions of the RAA. Registrars must contractually obligate all its Resellers to comply and enforce all RAA provisions. The Registrar will be held directly liable for any breach of the RAA a Reseller commits in which the Registrar does not remediate immediately. All Registrar resellers and third-party beneficiaries should be listed and reported to ICANN who shall maintain accurate and updated records.

Summary of Discussion
Such an amendment would work if a notice / cure period were added to the provision. There also needs to be additional clarity on the definition of "liability." The "reseller" term needs specificity as registrars employ resellers for multiple services. It was suggested that any liability be limited to cases where action was not taken within a reasonable time period following notification of the registrar.

It was discussed again that ICANN is not equipped to maintain the proposed list of resellers, and would therefore be out of compliance with the RAA.

Proposal No. 9
9) Registrars and all associated third-party beneficiaries to Registrars are required to collect and securely maintain the following data:

(i) Source IP address

(ii) HTTP Request Headers
(a) From
(b) Accept
 (c) Accept - Encoding
(d) Accept - Language
(e) User - Agent
(f) Referrer
(g) Authorization
(h) Charge - To
(i) If - Modified - Since

(iii) Collect and store the following data from registrants:
(a) First Name:
(b) Last Name:
(c) E - mail Address:

(d) Alternate E - mail address
(e) Company Name:
(f) Position:
(g) Address 1:
(h) Address 2:
(i) City:
(j) Country:
(k) State:
(l) Enter State:
(m) Zip:
(n) Phone Number:
(o) Additional Phone:
(p) Fax:
(q) Alternative Contact First Name:
(r) Alternative Contact Last Name:
(s) Alternative Contact E - mail:
(t) Alternative Contact Phone:

(iv) Collect data on all additional add - on services purchased during the registration process.

(v) All financial transactions, including, but not limited to credit card, payment information.

Summary of Discussion
Registrars did not question the spirit of what is trying to be achieved here. However there are questions about the details that would be collected. In fact, collection of data is one issue—storage of that data is another, and its transmission is yet another. Data transmission and storage of data not needed to provide the service often run contrary to EU privacy laws. A time limit for data storage would be useful.

Care should be taken with definition of "securely." Credit card data may need to be stored in a separate location. The room was unsure if this can be technically accomplished at a level that LEAs need.

Proposal No. 10
10) Each registrar is required to validate the following data upon receipt from a registrant:

(1) Technical Data
(a) IP addresses used to register domain names.
(b) E - mail Address
(i) Verify that registration e - mail address(es) are valid.

(2) Billing Data
(a) Validate billing data based on the payment card industry (PCI standards), at a minimum, the latest version of the PCI Data Security Standard (DSS).

(3) Contact Data
(a) Validate data is being provided by a human by using some anti - automatic form submission technology (such as dynamic imaging) to ensure registrations are done by humans.
(b) Validate current address WHOIS data and correlate with in - house fraudulent data for domain contact information and registrant's IP address.

(4) Phone Numbers

(i)   Confirm that point of contact phone numbers are valid using an
       automated system.
(ii) (ii) Cross validate the phone number area code with the provided
       address and credit card billing address.

<u>Summary of Discussion</u>
There was broad agreement in the ultimate goal of this proposal but an
acknowledgement that the economic, operational and technical challenges would be
great. Also, and equally importantly, against what data would registrars validate, and
how would it be secured without violating privacy laws?

<u>Proposal No. 11</u>
11) Registrar must provide abuse contact information, including the SSAC SAC 038
recommendations below:

- Registrars must prominently publish abuse contact information on their website and
  WHOIS.

   1. The registrar identified in the sponsoring registrar field of a Whois
       entry should have an abuse contact listed prominently on its web
       page. To assist the community in locating this page, registrars
       should use uniform naming convention to facilitate (automated and
       rapid) discovery of this page, i.e.,
       http://www.<registar>.<TLD>/abuse.html.
   2. Registrars should provide ICANN with their abuse contact
       information and ICANN should publish this information at
       http://www.internic.net/regist.html.

- The information a registrar publishes for the abuse point of contact should be
  consistent with contact details currently proposed as an amendment to Section 3.16
  of the RAA. Each contact method (telephone, email, postal address) should reach an
  individual at the Registrar who will be able to promptly and competently attend to an
  abuse claim; for example, no contact should intentionally reject postal or email
  submissions.

- Registrars should provide complainants with a well-defined, auditable way to track
  abuse complaints (e.g. a ticketing or similar tracking system).

<u>Summary of Discussion</u>
There was agreement in the room on this proposal.

<u>Proposed No. 12</u>
12) ICANN should require Registrars to have a Service Level Agreement for their Port 43
servers.

<u>Summary of Discussion</u>
The difficulty with this proposal is how to define a penalty for not meeting the SLA. There
was no objection to the concept, however.

Next Steps: Near-Term

Registrars and law enforcement agree to move forward with the following in the near term:

- Registrars to publish on their websites a valid physical address for receiving legal service
- Registrars to publish a contact for handling abuse complaints
- Contracted parties and law enforcement to continue meeting and discussing additional outcomes and most effective and practical method to achieve them (which may or may not entail RAA amendments)

Next Steps: Longer Term

- Agree with ICANN on parameters for enhanced due diligence for accreditation of registrars
- Develop template process for LEA to document and provide evidence of improper online behavior in the relevant country and according to the applicable national laws on which registrars can reasonably rely and act.
- Create a method for verification of identify of law enforcement contacting contracted parties requesting action.
- Adoption of the CICILE LEA database

A word about process

Registrars have heard that they are resistant to needed changes. However, registrars want to emphasize that they are seeking the most effective means to assist the community without needlessly disrupting their own operational stability.

The most effective step toward getting the assistance of registrars is to approach them and describe a problem and discuss ways to address it. Such a process will intelligently inform everyone involved as to the best path forward, and will prevent frustration by others when registrars helpfully point out the possible operational shortcomings of proposals.

In this instance, dialogue with registrars began following LEA proposals and their endorsement by the GAC and others. Registrars understand the current impatience of the community; however, it is better to directly address the operational issues now, when there is an opportunity to ensure thoughtful and correct execution, than risk further frustration later if policies are not adequately vetted.

Thanks

Registrars, registries and LEAs extend their heartfelt thanks to the European Commission for their hospitality and generosity in providing a forum for the productive and collegial discussions over the past two days.

Annex 5 -Modified Process B

1.   The GNSO Council requests that the ICANN Office of the General Counsel review the prioritized list of topics as set forth in the Final Report and identify any topics that would require consensus policy development rather than RAA contract amendment. The GNSO Council requests that the Office of the General Counsel complete and publish on the ICANN website the outcome of such review and identification not later than seventy-five (75) days after the date of this resolution.

2.   ICANN Staff will schedule a public consultation, to be held at the first ICANN public meeting that occurs after completion of the review in Step 1, to provide members of the ICANN community with the opportunity to articulate their support of and/or objection to the High and Medium Priority topics described in the Final Report.

3.   Within sixty (60) days after the public consultation described in Step 2, negotiations begin with the Negotiating Group consisting of ICANN Staff and the Registrar Stakeholder Group (as a whole).

4.   The Negotiating Group shall provide, for public comment, bimonthly written reports on the status and progress of the negotiations. Such reports shall include proposed text under consideration and identify items and text agreed upon by the Negotiating Group. Each bimonthly report shall identify the status of (a) topics identified in the Final Report as High or Medium Priority and that were not determined in Step 1 as requiring consensus policy development; and (b) proposed amendments put forth by any Stakeholder Group, Constituency, and/or Advisory Committee; and shall identify such topics, if any, that have been rejected by the Negotiating Group (collectively, the "Rejected Topics and Amendments").

5.   The Negotiating Group shall review public comments received and continue negotiations as necessary. Steps 4 and 5 shall repeat as necessary; provided, however, that the full final draft of the new RAA must be posted for public comment not later than March 4, 2013.

6.   Subject to the date requirement in Step 5, ICANN Staff and the Registrar Stakeholder Group shall determine when the full final draft of the new RAA is ready to be posted for public comment. The full final draft of the new RAA that is posted for public comment shall be accompanied by a detailed written explanation, approved by both Staff and the Registrar Stakeholder Group, that sets forth the basis for the rejection of all Rejected Topics and Amendments.

7.   The GNSO Council shall review the full final draft of the new RAA, consider public comments, and vote on approval of the draft new RAA. A Supermajority vote of the GNSO Council is required to approve the new RAA.

8.   If the GNSO Council approves the new RAA, the new RAA goes to Board for approval.

9.   If the GNSO Council does not approve the new RAA, the new RAA is sent back to the Negotiating Group with appropriate feedback for reconsideration. Repeat from step 7.

ANNEX 6- CATEGORIZATION OF AMENDMENT TOPICS

EXPLANATION OF THE CHART

The Chart below lists each of the High Priority Amendment Topics from the RAA Final Report, and from the Code of Conduct proposed by LE representatives, and suggests possible ways of approaching the topic.   Because there are multiple paths that can be adopted to achieve a new form of RAA, Staff invites the Registrars, and the representatives from the Law Enforcement community, to collaborate to identify which processes may be preferable, and most expedient, to bring about improvements to the RAA.

2009 RAA Process-   This column refers to topics for which a process could be followed that similar to that which was followed to achieve the 2009 RAA.   Specifically, this suggests: (1) negotiations between Staff/Registrars to identify topics which are acceptable, (2) a posting for public comment the proposed new form of RAA based on these discussions, (3) a follow-up negotiations to address public comments, (4) delivery of the updated Form of RAA to the GNSO Council for its approval, and (5) Board Approval of the New Form of RAA.

PDP- This column indicates that a PDP could be initiated by the GNSO Council to address the topic either to attempt to create a new consensus policy on the specific topic, because the topic reflects a substantive new policy change, or through a general "PDP on Contractual Conditions for the RAA", for items that may be less controversial.

Advisory- This column refers to topics that have the potential of being addressed through a Staff Advisory, to interpret existing obligations in the RAA.

	Categorization of RAA Amendment Topics				
	High Priority Topics				
No.	**Amendment Topic**	**2009 RAA Process**	**PDP**	**Registrar Advisory**	**Notes**
1	Prohibition on registrar cybersquatting	Yes	Yes	Yes	Consistent with obligations already in existence under RAA
2	Malicious conduct – registrar duty to investigate	Yes	Yes	No	Consistent with LE/Registrar discussions
3	Designation and publication of technically competent point of contact on malicious conduct issues, available on 24/7 basis	Yes	Yes	No	Consistent with LE/Registrar discussions
4	Registrar disclosure of privacy/proxy services made available in connection with registration and responsibility of registrar compliance by such services	Yes	Yes	No	Consistent with obligations already in existence under RAA
5	Obligations of privacy/proxy services made available by Registrars in connection with registration re: data escrow; Relay function; Reveal function	Yes	Yes	No	Consistent with LE/Registrar discussions

No.	Amendment Topic	2009 RAA Process	PDP	Registrar Advisory	Notes
6	Registrar responsibility for cancellation under appropriate circumstances of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal	Yes	Yes	Yes	
7	Define circumstances under which registrar is required to cancel registration for false Whois data and set reasonable time limits for registrar action	Yes	Yes	Yes	
8	Require PCI compliance in registration process	Yes	Yes	No	Consistent with LE/Registrar discussions
9	Define "reseller" and clarify registrar responsibility for reseller compliance for obligations	Yes	Yes	Yes	
10	Require greater disclosure of registrar affiliates/multiple accreditations	Yes	Yes	Yes	
11	Require greater disclosure of registrar contact information, information on form of business organization, officers, etc.	Yes	Yes	Yes	
12	Clarification of registrar responsibilities in connection with UDRP proceedings	Yes	Yes	Yes	Consistent with obligations already in existence under RAA Section 3.7.5.7--- advisory could define terms "Registrar HOLD," Registrar LOCK"

	Medium Priority Topics				
No.	Amendment Topic	2009 RAA Process	PDP	Registrar Advisory	Notes
1	Spell out "verification" process registrars are required to undertake after receiving report of false Whois data	Yes	Yes	Yes	Advisory could clarify requirements under Section 3.7.8
2	Require links to Whois Data Problem Reporting System on Whois results pages and on registrar home page	Yes	Yes	No	
3	Service Level Agreement on Whois availability	Yes	Yes	Yes	Consistent with LE/Registrar discussions
4	Registrar to disclose resellers and vice versa	Yes	Yes	No	
5	Expand scope of authority to terminate accreditation	Yes	Yes	No	
6	Require registrars to report data breaches	Yes	Yes	No	
7	Streamline arbitration process in cases of dis-accreditation	Yes	Yes	No	
8	Streamline process of adding new gTLDs to accreditation	Yes	Yes	No	
9	Registrar responsibilities for acts of affiliates	Yes	Yes	No	

No.	Amendment Topic	2009 RAA Process	PDP	Registrar Advisory	Notes
10	Staff to draft registrar code of conduct if registrars fail to do so by time certain	No	No	No	Staff and Registrars could commence Process to develop Code of Conduct referenced 3.7.1 on items where there is likelihood of achieving consensus in Registrar SG

	Additional Topics from LE Code of Conduct				
No.	Topic	2009 RAA Process	PDP	Registrar Advisory	Notes
I	General Commitment to Cooperate with LE investigations	Yes	Yes	No	
II.1.a	Use of Privacy/Proxy Registrations- ICANN Accreditation Program for Privacy/Proxy Services	Yes	Yes	No	
II.1.b.	Publishing authentic WHOIS for proxy/privacy customer if found in violation of terms of service	Yes	Yes	Yes	Similar to High Priority Topic # 6 above
II.2	Prohibition of Certain Illegal, Criminal or Malicious Conduct	Yes	Yes	No	
II.3	Valid Physical Address to be Published	Yes	Yes	Yes	Could also be covered under an advisory on Section 3.16
II.4	Valid Officer Data to be Published	Yes	Yes	No	
II.5	Public Disclosure of Affiliates	Yes	Yes	No	Similar to High Priority Topic # 10 above

No.	Topic	2009 RAA Process	PDP	Registrar Advisory	Notes
II.6	Notice to ICANN of Certain Changes	Yes	Yes	No	
II.7	Maintenance of Business Licenses	Yes	Yes	No	
II.8	Publication of Abuse Point of Contacts	Yes	Yes	No	
II.9	Service Level Agreement for Port 43 WHOIS Access.	Yes	Yes	No	
IV	Further Assurances	Yes	Yes	No	