Preliminary GNSO Issue Report on the Registrar Accreditation Agreement Amendments

STATUS OF THIS DOCUMENT

This is the Preliminary Issue Report on the Registrar Accreditation Agreement Amendments requested by the ICANN Board at the Dakar ICANN Meeting. This report is to be published for public comment for not less than thirty (30) days, and is to be followed by a Final Issue Report to be published after the closure of the public comment forum.

SUMMARY

This report is submitted to the GNSO Council in response to a request received from 1) the ICANN Board pursuant to a motion carried on 28 October 2011, and 2) the GNSO Council in response to a motion carried during the 6 October 2011 GNSO Council teleconference meeting.

TABLE OF CONTENTS

I. Executive Summary

This Preliminary Issue Report is published in order to commence an ICANN Board directed GNSO policy development process (PDP) to consider “meaningful amendments to the Registrar Accreditation Agreement (RAA) in the global public interest with the twin goals of registrant protection and stability in mind.”[1] In Dakar, the Board conveyed its sense of urgency on this issue, noting that law enforcement agencies and a GNSO working group have developed a list of specific recommendations for amending the RAA to provide greater protections for registrants and reduce abuses. Observing that no action has been taken on these recommendations, the Board stated that it “requires action” on these RAA initiatives and directed the commencement of immediate negotiations between ICANN and the contracted parties to rapidly develop a set of amendments for consideration at ICANN’s meeting in Costa Rica in March 2012.

Recognizing that not all of the proposals for RAA amendments may be included in the revised RAA that is anticipated through these negotiations, the Board has requested an Issue Report in order to commence a policy development process on the “remaining items” so that they can be considered by the GNSO “as a matter of urgency.” As a result, this Preliminary Issue Report summarizes and categorizes each of the 24 proposed RAA amendment topics as a required step before for the GNSO Council can commence a PDP on these topics as requested by the Board. Staff has confirmed that the Proposed Amendment Topics are within the scope of the ICANN policy process and the GNSO.

A Public Comment Forum will be conducted on this Preliminary Issue Report, and will be followed by the publication of the Final Issue Report. It is expected that the GNSO Council will commence a PDP, as required by the Bylaws, following the publication of the Final Issue Report.

[1] See the Board Resolution (2011.11.10.18.32) from the Dakar Meeting.

Details of the proposed amendment topics are listed in Annex 2 (the "Proposed Amendment Topics") of this Preliminary Issue Report. During the Public Comment Forum, the ICANN community is invited to comment on any of these Proposed Amendment Topics or any other aspect of this Preliminary Issue Report.

II. Objective

This Preliminary Issue Report[2] is published in response to the Board Resolution (2011.11.10.18.32) in Dakar (the "Dakar RAA Resolution") regarding amendments to the Registrar Accreditation Agreement (Annex 1). In the Dakar RAA Resolution, the Board acknowledged that continuing to evolve the RAA is an important element of a program to protect registrants and safeguard the stability of a single interoperable Internet. The Dakar RAA Resolution also directed negotiations to be commenced immediately, so as to result in proposed amendments to be provided for consideration at ICANN's meeting in Costa Rica in March 2012.

The Dakar RAA Resolution clarified that the subject of the negotiations is to include the recommendations made by law enforcement, those made by the GNSO RAA drafting team[3] (RAA Final Report) as well as other topics that would advance the twin goals of registrant protection and DNS stability. This resolution further requested the creation of an Issue Report to undertake a GNSO policy development process (PDP) as quickly as possible to address remaining items suited for a PDP.

In its rationale for the Dakar RAA Resolution, the Board conveyed its sense of urgency on this issue. It noted that although law enforcement agencies and a GNSO working group have developed a list of specific recommendations for amending the RAA to provide greater protections for registrants and reduce abuses, no action has been taken on these recommendations. Direct negotiations between the contracted parties are a way to rapidly develop a set of amendments for consideration. However, for the benefit of the ICANN community, the Board requested an issue report to explore the policy

[2] This Preliminary Issue Report follows the new PDP format adopted by the ICANN Board at its 7 December 2011 meeting. The new PDP model accommodates a more flexible time-frame and consultative approach to delivering the Issue Report, and introduces the concept of a "Preliminary" Issue Report to be published prior to the "Final" Issue Report.

[3] The Final Report on Proposals for Improvements to the RAA is posted at: http://gnso.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf.

alternatives for developing and making binding changes to the RAA. The Board also recognized and accepted the GAC Communiqué statement that the ICANN Board should take the necessary steps to ensure that ICANN's multi-stakeholder process effectively addresses the GAC-endorsed proposals in this regard as a matter of extreme urgency.

In keeping with this urgent mandate, this Preliminary Issue Report is written to address all of the recommendations from the law enforcement community, and all of the topics designated as "High Priority" and "Medium Priority" in the RAA Final Report.[4] Although Staff expects that many of these topics will be addressed through the RAA negotiations that will be conducted between ICANN and registrars, it is impossible to predict at present which amendment topics will ultimately be resolved through the agreement of terms in the ICANN/gTLD registrar negotiations. Rather than introduce additional delays by waiting for the conclusion of the negotiations to commence new policy work, this Preliminary Issue Report attempts to address all of these recommendations, while some may be resolved prior to the PDP.

This Report is designated as "preliminary" to allow for Community input and dialogue prior to the publication of the Final Issue Report. A Public Comment Forum on this Preliminary Issue Report will be opened for at least 30 days.

[4] As indicated by the chart in Annex 2, several of the LEA recommendations are incorporated in the "High Priority" and "Medium Priority" topics.

III. Background

The Registrar Accreditation Agreement (RAA) is the contract that governs the relationship between ICANN and its accredited registrars (a directory of accredited registrars can be found at http://www.internic.net/regist.html). Its provisions also may have impacts on registrants and other third parties involved in the domain name system.

Because the domain name market has undergone changes in recent years and the number of ICANN accredited registrars and domain name registrations have grown significantly, all parties affected recognize that amendments may need to be made to this important agreement from time to time.

The RAA was last amended by the ICANN Board in May, 2009. At the time, some community members expressed their support for the 2009 RAA while others insisted that it had not gone far enough to address concerns.[5]

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) was submitted to the GNSO Council on 18 October 2011 and 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 proposed RAA

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

improvements forward, reflecting the differences within the community on both substantive and process issues.[6]

Separately, over the past two years, representatives from the law enforcement (LE) community and registrars have held several meetings to discuss law enforcement proposals to address their concerns with regard to e-crime 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 diligence on registrars, and a proposed Registrar Code of Conduct.[7] The Law Enforcement Due Diligence Recommendations for ICANN-Seoul submitted for discussion at the ICANN Seoul Meeting in October 2009 ("LE Seoul Recommendations") were endorsed by the GAC in Brussels, and were subsequently highlighted in various GAC communiqués.[8] Apart from the GAC-LE discussions, these proposals were discussed separately between LE and registrars in order to determine whether the proposals were practical to implement. These meetings between LE representatives and a group of registrars were aimed at encouraging Registrar-LE dialogue, evaluating LE proposals,[9] and producing a voluntary cooperation model outside of ICANN's processes and policies.[10] However, these independent efforts to produce a voluntary LE/registrar cooperation model did not result in substantive changes to the RAA.

[6] 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.

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

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

[9] The registrars' responses to the LE proposals are posted at: see http://gnso.icann.org/mailing-lists/archives/registrars/msg05877.html

[10] More details on the substance of the proposals evaluated can be found in the Registrar Stakeholder Group Statement attached to the Staff Discussion Paper as Annex 4, and the Code of Conduct, attached as Annex 3 proposed by the LE representatives, which was discussed in Singapore, and referenced in the GAC Singapore Communiqué. The Staff Discussion Paper is posted at: : http://gnso.icann.org/issues/final-raa-discussion-paper-13oct11-en.pdf

On 6 October 2011, the GNSO Council passed a motion (Annex 3) submitted on behalf of the Registrar Stakeholder Group to address some of the LE recommendations through a new policy development process (PDP). Because of overlap in topics identified in this GNSO Council motion with the topics referenced by the Board in its Dakar RAA Resolution, this Preliminary Issue Report is also intended to address this request.

IV. Commencement of Negotiations on the RAA

Prior to Dakar, Staff published a Discussion Paper on the Next Steps for the RAA[11] recommending the immediate commencement of bilateral negotiations between ICANN and its accredited registrars.

In response, the Registrars Stakeholder Group and ICANN announced the immediate commencement of negotiations on the RAA at the ICANN meeting in Dakar.[12] The negotiation process will run continuously with the intention to arrive at proposed amendments to the RAA prior to ICANN's Costa Rica Meeting. Registrars and ICANN plan to update the community regarding the substance and progress of negotiations on a regular basis, through use of the RAA Negotiations Community Wiki created to provide detailed information on each negotiation session conducted, and the issues explored.[13]

The publication of this Issue Report in response to the Dakar RAA Resolution is not intended to delay or supplant the bilateral negotiations, which are expected to address many of the amendment topics discussed below. Instead, this Report is published contemporaneously with the commencement of negotiations, to allow a more expeditious review of potential amendment topics that are not addressed within the negotiations, and for those that proceed to policy development, if appropriate. The one or more PDPs that may result from the Board’s Dakar RAA Resolution may run in parallel to the RAA negotiations so that the ICANN community can be assured that all of the topics identified below will receive adequate consideration, and will be dealt with “extreme urgency” as directed by the Board. To streamline the multiple tracks of work, it is suggested that once a determination has been made that a specific amendment

[11] See: http://gnso.icann.org/issues/final-raa-discussion-paper-13oct11-en.pdf

[12] The announcement of negotiations is posted at: http://www.icannregistrars.org/calendar/announcements.php

[13] The ICANN Community Wiki is posted at: https://community.icann.org/display/RAA/Negotiations+Between+ICANN+and+Registrars+to+Amend+the+Registrar+Accreditation+Agreement;jsessionid=63926D7F22EA5DE9CAFEB8B84396F63E

topic will be addressed in the negotiations, that issue should be “removed” from further consideration under the PDP.

V. Advice from ICANN Advisory Committees on the RAA

Several endorsements and communiqués from ICANN Advisory Committees related to the Registrar Accreditation Agreement amendments have been provided. These include:

A. Statements from the At-Large Advisory Committee (ALAC)

During its meeting of 25 May 2010, the At-Large Advisory Committee (ALAC) by consensus endorsed a draft version of the Initial Report on Proposals for Improvements to the Registrar Accreditation Agreement.

In addition, ALAC released a statement[14] to the ICANN Board on 2 May 2011 on the RAA negotiations, calling for more transparency and accountability with regard to the RAA negotiations. The ALAC noted that "while the RAA has the form of a contract between the registrars and ICANN, this should not mean that only the directly contracted parties should be part of the discussion…." The ALAC observes that ICANN uses contracts as a tool to formalize what results from a larger participatory process; therefore, in the view of the ALAC, the contract is the tool, not the framework. ALAC perceives this issue to be fundamental to ICANN's function, perception and credibility as a multi-stakeholder, bottom-up institution.

B. Communiqué's from the Government Advisory Committee (GAC)

In its June 2010 Brussels Communiqué, the GAC issued its endorsement of the law enforcement proposals for amendments to the RAA Brussels Communiqué. Specifically, the Brussels Communiqué states that:

[14] https://community.icann.org/download/attachments/13862605/AL-ALAC-ST-0511-1+ALAC+Statement+on+the+RAA+Negotiations+-+EN.pdf

> "An absolute majority of GAC members made the following statement:
>
> 1. The GAC encourages the Board, the RAA Working Group and registrars to work with law enforcement agencies to address their concerns and implement necessary changes without delay.
>
> 2. Following from the GAC's Nairobi Communiqué, the GAC requests an update of progress on consideration of these proposals, including the Board's consideration of the due diligence recommendations.
>
> 3. Based on the deliberations in Brussels and the previous meetings, the GAC endorses the proposals from law enforcement agencies to address criminal misuse of the DNS, noting that implementation of these proposals must respect applicable law and respect all requirements concerning the processing of personal data, such as privacy, accuracy and relevance.
>
> Some countries felt that further efforts need to be deployed to clarify these proposals."

The GAC's June 2011 Singapore Communiqué states:

> "The GAC, together with representatives of law enforcement agencies (LEAs) from several GAC members, engaged with the Generic Names Supporting Organization (GNSO) Registrar Stakeholder Group on the status of LEA efforts to advance a "code of conduct" or "agreed best practices", and reinforced the critical importance of demonstrating concrete and effective support for LEA objectives to include a timetable of implementable actions. The GAC welcomes the registrars' offer to identify any substantive implementation issues with any unresolved LEA recommendations, for further dialogue with the GAC."
>
> "The GAC recalls its endorsement of LEA recommendations for due diligence and amendments to the Registrar Accreditation Agreement in June 2010, and urges the Board to support actions necessary to implement those recommendations as a matter of urgency."

The GAC's October 2011 Dakar Communiqué states:

> "In recent years, the Internet has grown to have over two billion users and be a significant contributor to the global economy.
>
> Cyber-crime is a growing threat to the security and stability of the Internet, with broad and direct public policy impacts. Recent estimates suggest that the direct financial impact of cyber crime is extremely significant.

Law enforcement agencies have identified a series of specific problems which are limiting their ability to address this growing problem.

As part of this, law enforcement agencies have identified specific areas of concern in the ICANN context, relating to contractual weaknesses and a lack of necessary due diligence.

To address these urgent problems, in 2009 law enforcement agencies made 12 concrete recommendations to reduce the risk of criminal abuse of the domain name system.

These recommendations were informally socialized with the registrar community, the GAC, and with ICANN compliance staff over the course of several months, before the GAC advised the Board in its Brussels communiqué that it formally endorsed the recommendations.

Direct exchanges between law enforcement agencies and registrars continued in September 2010 in Washington D.C., in February 2011 in Brussels, and during the March and June 2011 ICANN meetings.

As a complement to the June exchanges in Singapore, the GAC urged the Board to support actions necessary to implement those recommendations as a matter of urgency.

To date, none of the recommendations have been implemented, and the risks remain. The GAC therefore advises the ICANN Board to take the necessary steps to ensure that ICANN's multi-stakeholder process effectively addresses these GAC-endorsed proposals as a matter of extreme urgency."

VI. Community Input on Potential RAA Amendment Topics

The RAA Final Report was produced by a joint GNSO and ALAC effort that took place over an 18 month period, and included members of the GNSO (including members of the Registrar Stakeholder Group) and the At-Large communities. ICANN Compliance Staff also actively contributed to the RAA DT's deliberations and published Staff Notes describing amendment topics that could enhance its compliance activities.[15]

To accomplish its task, the RAA DT divided into two subteams, each working independently to produce its recommendations. On 28 May 2010, the RAA DT published its Initial Report on Improvements to the RAA and opened a public comment period to solicit input from the broader ICANN community on the RAA.[16] The subteams then took this comment into account when producing a Final Report.

The RAA Final Report states that its recommendations were endorsed by a consensus of the respective subteams on (i) the proposed form of a Registrant Rights and Responsibilities Charter, and (ii) describing the potential topics for additional amendments to the RAA. For the proposed amendment topics, the subteam assigned priority levels to each of the amendment topics including within the RAA Final Report. The amendment topics included in the RAA Final Report that were designated as "High Priority" or "Medium Priority" are included in Annex 2 as Proposed Amendment Topics to be negotiated by the RAA negotiation teams or to be the subject of a PDP in response to the Dakar RAA Resolution.

Because no consensus was achieved on the proposal for next steps for the GNSO Council to consider in determining whether to recommend a new form RAA to be adopted by

[15] The Staff Notes Document dated October 14, 2009, is included in Annex F of the RAA Final Report.
[16] For information on the Public Comment Forum on the Initial Report, please see: http://www.icann.org/en/public-comment/public-comment-201007-en.htm#raa-improvements2010

the ICANN Board, the RAA Final Report described two alternative processes, one that received the strong support of the RAA DT, and one that was supported by a minority. Neither of these processes was approved by the GNSO Council.

The RAA Final Report clarified that the RAA DT was not asked, nor did it attempt, to achieve a consensus that these proposed amendment topics *should be* included in a new form RAA. Instead, the list is intended to serve as a *starting point* for additional topics to be considered, debated, and either accepted or rejected to be part of a new form of RAA for consideration by the ICANN Board.

VII. Impact of the RAA on ICANN

As a party to the RAA, ICANN is responsible for enforcing its terms. At times, there has been a general misunderstanding regarding the scope of enforcement actions that can be brought by ICANN in response to complaints from registrants and others. ICANN often receives complaints for registrar misconduct for which no remedy is available under the RAA. However, ICANN's authority to take action against a registrar is limited by the terms of its contract, the RAA. By amending the RAA or adopting a new form of RAA to address issues such as those raised by the LE representatives and the RAA DT in the RAA Final Report, ICANN would benefit by having greater clarity to support enhanced compliance activities. These enhanced terms are all the more important as ICANN prepares for the launch of the New gTLD Program, and the expected increase in new registrations, registries and registrants from all over the world, in multiple languages and scripts. Many of the principles identified in the new gTLD program, such as those addressing malicious conduct, cybersquatting, and enhanced verification, are equally applicable to the RAA.

Through a round of RAA amendments approved in 2009, ICANN has a more robust contractual framework which has achieved registrant protections and ICANN's enforcement capabilities. Further, the GNSO has resolved to continue to improve and innovate in the area of registrant protections and the RAA. The potential RAA amendments presented in this Preliminary Issue Report, and the policy processes to be initiated by the GNSO Council, are intended to enhance ICANN's and the registrars' ability to attain compliance with the contract.

VIII. Discussion of Possible Options for Amending the RAA and Producing a New Form of RAA

There are several ways to produce amendments to the RAA or a new form of RAA, as described more generally in the Staff Discussion Paper published prior to Dakar.[17] Set forth below is an analysis of the possible policy paths that the GNSO Council can pursue to evaluate the list of proposed amendment topics that are identified on Annex 2 (Proposed Amendment Topics).

PDP on New Policy Initiatives. Some of the Proposed Amendment Topics reflect new policy initiatives that could be explored through formal PDP processes on the specific topic. 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. Each of these Proposed Amendment Topics have the potential, depending upon the details of the final recommendations, to become binding "consensus policies" to become enforceable on all of the registrars immediately.

PDP on Contractual Conditions for the RAA. Some of the Proposed Amendment Topics may be more easily 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.[18] That effort led to a GNSO recommendation that was adopted by the ICANN Board in 2008.[19] Many of the Proposed Amendment Topics can appropriately be

[17] The Staff Discussion Paper on Next Steps to Produce a New Form of RAA is posted at: http://gnso.icann.org/issues/final-raa-discussion-paper-13oct11-en.pdf.

[18] 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.

[19] 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+gTLDs+%28PDP-Feb06%29.

included in a PDP on Contractual Conditions for the RAA, and can be effective immediately on all registrars, if the topics are appropriate for consideration as "Consensus Policies" under the RAA.

Determining whether an Amendment Topic can be a binding "Consensus Policy."

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." 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[20] 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 in section 4.2 and in other sections of the RAA.

The chart included on Annex 2 identifies the Proposed Amendment Topics, which includes the topics designated by the RAA DT as "High Priority" and "Medium Priority," the topics from the LE community as included in their initial list of 12 recommendations to the RAA DT, and the LE Seoul Recommendations, and highlights whether the topics would be in scope for the GNSO Council. Annex 2 does not definitively categorize these topics as "within the picket fence" because more specificity is required in order to make this determination. Instead, it references the Section of the RAA that could be

[20] 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.

applicable to the specific topic to make the resulting amendment an enforceable "Consensus Policy."

An enforceable Consensus Policy may take the form of a stand-alone policy that becomes part of the obligations that a registrar is subject to under the RAA, or can be in the form of an amendment to the RAA that changes the terms of the RAA itself. The degree of specificity to determine if the recommendation will become "binding" on a registrar is generally not attained until the details are discussed. 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 2, each of the Proposed Amendment Topics is a potential candidate for a Policy Development Process. At the end, some aspects might be "within the picket fence" while certain aspects of the same topic might be outside it.

Alternatives for producing "binding" changes through ICANN's Policy Processes.

In its rationale for the Dakar RAA Resolution, the Board noted that:

"For the benefit of the ICANN community, the Board is also requesting an issues report to explore the Policy alternatives for developing and making binding changes to the RAA. The Board also recognizes and accepts the GAC Communiqué statement that the ICANN Board to take the necessary steps to ensure that ICANN's multi-stakeholder process effectively addresses these GAC-endorsed proposals as a matter of extreme urgency."

The PDP could produce "binding" changes as follows:

- **Adopting a Consensus Policy** - which could include actual language for the RAA to address the recommendation. This would be similar to the outcome achieved in 2004 when the WHOIS Marketing Restriction Policy was adopted as a Consensus Policy that included specific language to include in the RAA.[21]

- **Recommending a New Form of RAA** - Instead of coming up with individual amendments to the RAA, the PDP could produce a new Form of RAA, following the procedure identified in Section 5.4 of the RAA, which addresses ICANN's right to substitute an updated agreement upon renewal. This would be similar to the process followed by ICANN in the adoption of the 2009 Form of RAA.
- **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. The PDP could recommend, for example, that ICANN adopt additional text in a "New gTLD Appendix" to address the new language from the Proposed Amendment Topics that achieve consensus.
- **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 suitable for consideration for inclusion in a Code of Conduct as referenced in the RAA. The PDP could recommend that ICANN take the steps necessary to see that a Code of Conduct is adopted by the registrars

[21] For more details on the WHOIS Marketing Restriction Policy, see http://www.icann.org/en/registrars/wmrp.htm

under the existing Section 3.7.1, assuming that a consensus is achievable from the Registrar Stakeholder Group.

IX. Overlap of Issues Raised by Proposed Amendment Topics with Other Policy Efforts

Many of the Proposed Amendment Topics address issues for which the GNSO Council is currently undertaking, or is considering initiating, policy related work. Because this effort to amend the RAA is to occur on an expedited basis as directed by the Dakar RAA Resolution, it is unclear whether any of these projects will be impacted. Staff recommends that the GNSO Council consider whether any of these pending projects or future projects should be revised or suspended pending the outcome of the RAA negotiations and the RAA related PDPs being initiated as a result of the Dakar RAA Resolution.

A. Law Enforcement Related Topics from the GNSO Council Motion.

As previously described, the GNSO Council has approved a motion (Annex 3) (GNSO RAA Motion) to consider certain of the law enforcement related RAA amendment topics. This motion also included additional policy details to be considered beyond the original law enforcement request which raise issues for the GNSO Council to consider.

For example, the GNSO RAA Motion includes a call for law enforcement agencies to "provide, within six months of the date of approval of this policy by the ICANN Board and via the general advice of the GAC to the Board, their recommendations for a database and identification system that allows for expedient identification to a registrar of a law enforcement agency, and verification of the contacting party as a law enforcement agency upon that agency's first contact with a registrar."

Staff interprets this portion of the GNSO RAA Motion as leading to advice to the Board that ICANN reach out to the LE community to determine if there is a way to develop a database or means of verifying law enforcement personnel for the purpose of accessing the registrar related information. ICANN does not have the authority to require law enforcement agencies to create a database or identification system, but can certainly undertake an effort to consult the LE community regarding whether such a system exists or can be created. Whether the LE community would like to assist in this endeavor would be purely voluntary.

As part of the public comment forum, Staff is interested in receiving input from experts in the ICANN community on whether such a system already exists or could be created.

B. WHOIS and Related Proposals

The list of specific recommendations for amending the RAA includes a number of WHOIS and related topics that relate to pending studies of WHOIS that are underway. In this section of this Report, we examine and identify which RAA proposals might be informed by or dependent on findings of these WHOIS studies or likely to be significantly shaped by study experiences. There are also several WHOIS-related proposals that would likely NOT be impacted by pending study results. In determining the breadth and scope of any future PDP on WHOIS, the community may want to consider first those recommendations that will not likely be impacted by study results, holding off on recommendations that are likely to be informed materially by study results.

As background, in the last few months, at the request of the GNSO Council, Staff has initiated four major studies of WHOIS, each of which will take over a year to complete. The decision to proceed with studies of WHOIS stemmed from years of policy debate about gTLD WHOIS, culminating in a lengthy policy debate in 2007 about whether current policies could be improved by implementing an “Operational Point of Contact,” or “OPOC.” The concept of the OPOC role was to act as an intermediary to “improve the privacy aspects of WHOIS for natural persons and the ability of legitimate parties to respond in a timely manner against fraud and other illegal acts by certain Registrants acting in bad faith".[22] In rejecting the OPOC proposal, the GNSO Council decided instead in October 2007 to initiate fact-based studies of WHOIS to provide a foundation for further policy making. The WHOIS studies initiated this year were selected by the Council from more than 40 study proposals as topical areas that would benefit the most from thorough data gathering and analysis before initiating further policy development. The four studies currently underway are examining the following:

1. WHOIS "Misuse" -- This year-long study, launched in June 2011, examines the extent to which public Whois contact information for gTLD domain names is misused to address harmful communications such a phishing or identity theft.
2. Whois Registrant Identification Study -- This year-long study, just launched this month, uses Whois to classify entities that register gTLD domain names, including natural persons, legal persons, and Privacy and Proxy service providers.
3. Whois Privacy and Proxy Services Abuse Study -- This year-long study (not yet launched) will examine the extent to which gTLD domain names used to conduct illegal or harmful Internet activities are registered via Privacy or Proxy services to obscure the perpetrator's identity. The study will methodically analyze a large, broad sample of domains associated with various kinds of illegal or harmful Internet activities. It will measure how often these alleged "bad actors" abuse Privacy/Proxy services, comparing rates for each kind of activity to overall Privacy/Proxy rates. If those rates are found to be significant, policy changes may be warranted to deter Privacy/Proxy abuse.
4. Whois Privacy and Proxy Relay and Reveal Survey -- This four-month survey will determine the feasibility of conducting a future in-depth study into communication Relay and identity Reveal requests sent for gTLD domain names registered using Proxy and Privacy services. If deemed to be feasible, an in depth study would be conducted. The pre-study survey should be completed in

[22] See: Final Outcomes Report of the WHOIS Working Group, 20 August 2007.

January 2012, but a full study, if approved, would likely take close to one year to complete following that decision.

Staff believes that the following RAA related proposals might be informed by or dependent on findings of the WHOIS studies currently underway:

- <u>Registrar Obligations A.9 - Registrar code of conduct</u>: Recommendation 2 (issues to be included in a possible Code of Practice) would be informed by study 3 (Abuse) findings, which will shed light on how often WHOIS data for abusive domain names turns out to be inaccurate or otherwise unusable (bullet 1, requirement to cancel a registration if inaccurate WHOIS information is not corrected), including those used for cybersquatting (bullet 4). So, knowing whether this occurs say 10% or 80% of the time would give more or less weight to this recommendation.
- <u>Privacy and Proxy Services B.1 [or B.2] - Obligations related to relay and reveal functions</u>: Recommendation B.1# 11 [or B.2 RAA DT #4] could be significantly informed by study 4 (Proxy and Privacy Relay and Reveal) ***<u>full-study</u>*** findings. If approved, the full Privacy Relay and Reveal study would analyze actual relay and reveal requests sent for Privacy and Proxy-registered domains to explore and document how they are processed and identify factors that may promote or impede timely communication and resolution. Currently, each Proxy or Privacy service provider has its own independently-developed practices for handling such requests. There is no common format for submitting these requests and no central repository for tracking them. The highly diverse and distributed nature of these practices has made it difficult to even assess the effectiveness of related ICANN policies. The objective of this full study would therefore be to help the ICANN community better understand how communication relay and identity reveal requests sent for Privacy/Proxy-registered domain names are actually being handled today. If policy discussions were to begin before study results are available,

it may be difficult to institute a process without assessing how relay and reveal requests are currently handled, how parties current interpret actionable harm, how long requests currently take, etc.

- WHOIS C.3 – Define requirements to cancel registrations for false WHOIS data: Recommendation 2 may be informed by study 3 (Privacy and Proxy Abuse) findings (in addition to the 2010 NORC WHOIS Accuracy study findings) in the sense that these studies might be viewed as pilots for verification processes. They could show what works, what does not, and quantify associated costs or barriers. Recommendation 1 also may be informed by study 2 (Registrant Identification) in that it will show how contact information is used by various entities, which could have bearing on what it really means to provide accurate contact information.
- WHOIS C.4 Verification: As for #C.3 above, Recommendation 1 may be informed by study 3 (Abuse) and the verification processes considered in the NORC WHOIS Accuracy study. (See: Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information: http://www.icann.org/en/announcements/announcement-3-15feb10-en.htm).

In sum, study results will be useful to inform policy discussions, and given the financial and resource commitment allocated and the value that the community expects study results to contribute, in Staff's view, policy work on the five topic areas related to the studies may be initiated, but should not concluded, prior to the publication of the study results. Policy discussions on gTLD WHOIS issues unrelated to anticipated study findings could be considered expeditiously by the community as explained further in Section XI below.

In addition to the GNSO's policy work on WHOIS, the GNSO Council should take note of the work recently conducted by the WHOIS Review Team (WHOIS RT). The WHOIS RT was established by the ICANN Board in response to the Affirmation of Commitments to review the effectiveness of ICANN's WHOIS policies. On 5 December, 2011, the WHOIS RT's Initial Report was posted for public comment,[23] and includes a series of recommendations to amend the WHOIS related obligations as listed in the RAA. Due to the overlap of issues related to WHOIS, Staff believes that a PDP on WHOIS should include evaluation of these additional RAA recommendations produced by the WHOIS RT.

C. UDRP

One of the topics identified as relevant to a PDP on the UDRP, which is currently under consideration by the GNSO Council, and which is also part of one of the RAA amendments,[24] relates to registrar obligations in relation to the locking/unlocking of a domain name that is subject to UDRP proceedings.

D. Uniformity of Contracts

The GNSO Council is currently considering commencing policy work based on the recommendations from the Registration Abuse Policies Working Group (RAPWG) pertaining to the uniformity of contracts issue. In response to recommendations in the RAPWG Final Report,[25] the GNSO Council requested an Issue Report to evaluate whether a minimum baseline of registration abuse provisions should be created for all in-scope ICANN agreements, and if created, how such language would be structured to address the most common forms of registration abuse. The release of the Preliminary Issue Report on Uniformity of Contracts is expected December 2011, and will include a

[23] The WHOIS DT Public Comment Forum on its Initial Report is available at: http://www.icann.org/en/announcements/announcement-05dec11-en.htm

[24] Item A-6: Clarification of registrar responsibilities in connection with UDRP proceedings

[25] The RAPWG Final Report is posted at: http://gnso.icann.org/issues/rap/rap-wg-final-report-29may10-en.pdf

discussion of the RAP-WG history, uniformity research, successful industry initiatives, and other content relative to registration abuse provisions among agreements. The scope of that report, and any PDP if initiated, is expected encompass the Registry Agreements, the Registry-Registrar Agreements, the RAA, and Registration Agreements.

Although the Uniformity of Contracts Issue Report will likely include a review of the RAA for the purposes of determining whether to require a minimum baseline for abuse provisions in the registration agreements with its registrants, Staff suggests that this work continue to be evaluated separately from the RAA Amendment negotiations and the PDP arising out of the Dakar RAA Resolution. In addition to the scope being greater than just the RAA, the foundational work required to understand how minimum registration abuse provision baselines would be structured and their corresponding impacts has not been accomplished. As a result, it may be preferable to have the GNSO Council consider a stand-alone Issue Report and PDP on this issue, which would address issues applicable to both registrars and to registries, and each of their agreements previously mentioned.

However, should the RAA negotiation teams reach agreement on the possible inclusion of a baseline provision regarding abuse for the RAA, the GNSO Council could consider revising the scope of any PDP on the Uniformity of Contracts Issue to take into account the outcome of the RAA negotiations.

E. Efforts to Develop Best Practices for Addressing Malicious Use of Domain Names

Acting on one of the recommendations of the Registration Abuse Policies (RAP) Working Group, the GNSO Council requested ICANN Staff prepare a discussion paper on best practices for registries and registrars to address registration abuse. The discussion paper which was submitted by ICANN Staff on 28 September 2011 outlines a number of issues that need to be addressed in moving forward with this topic such as the development of a framework for the development, maintenance and promotion of best practices in an ICANN context as well as a preliminary inventory of current or proposed best practices. Certain practices that were highlighted in this discussion paper, such as for example, providing a dedicated abuse contact, are also part of the proposed RAA amendments. However, as it is recommended that further work be carried out first on developing the actual framework for best practices, it is not likely that there will be a direct overlap in activities. Nevertheless, any issues that are brought up in the context of the RAA discussions but which are not addressed as part of the RAA amendments or a PDP, might be considered suitable for the best practices effort, should the GNSO Council decide to move forward with it.

X. Freedom of Expression Impact

The GNSO RAA Motion calls for a "freedom of expression" impact analysis with regard to the LE recommendations. This request was introduced by the Non-Commercial Stakeholder Group to highlight the importance of analyzing whether the LE recommendations could have a potentially adverse impact on the freedom of expression of registrants who may be customers of the registrars to which a law enforcement related inquiry might be directed.

As noted by Wendy Seltzer:[26] "domain names are often tools of individual and group expression; not so much through expressive content of the strings themselves, but through the speech hosted at a domain, the conversations carried on through URLs and hyperlinks, and the use of domains to route email and other messaging. Domain names provide stable location pointers for individuals' and groups' online speech; as such, they also present possible chokepoints for censorship and suppression of speech." She further notes that "in the specific instance of responding to law enforcement requests for the publication of registrar contact information, the potential impact is indirect but not insubstantial. In response to law enforcement requests for "registrar cooperation in addressing online crime," the GNSO RAA Motion considers a requirement that registrars "must publish on their respective web sites e-mail and postal mail addresses to which law enforcement actions may be directed."

Ms. Seltzer suggests that if there is a way to be "sure that the requests would relate only to activity universally agreed to be criminal, from law enforcement agencies following due process of law and respecting human rights, the proposed requirement would be uncontroversial. As legal regimes and their approaches to human rights are not uniform, we cannot make that blanket assumption. The contacts could be used to censor."

[26] See Wendy Seltzer's blog posted at: http://wendy.seltzer.org/blog/archives/2011/11/04/icann-the-stakes-in-registrar-accreditation.html

Ms. Seltzer further clarifies that the intent is not to interfere with legitimate law enforcement. She suggests that explicit procedure and limitations need to be developed so that “these contact points do not become points of control through which registrars can be pressured into removing domains that provide access to critical or “inharmonious” speech.”

Staff is interested in hearing from the ICANN community on proposals for addressing the concerns of “freedom of expression” in the Public Comment Forum that may be associated with the LE recommendations described in the Proposed Amendment Topics.

XI. STAFF RECOMMENDATION

Scope

In determining whether the issue is within the scope of the ICANN policy process and the scope of the GNSO, Staff and the General Counsel's office have considered the following factors:

Whether the issue is within the scope of ICANN's mission statement

The ICANN Bylaws state that:

> "The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:
>
> 1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are
>
> a. domain names (forming a system referred to as "DNS");
> b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and,
> c. protocol port and parameter numbers.
>
> 2. Coordinates the operation and evolution of the DNS root name server system.
>
> 3. Coordinates policy development reasonably and appropriately related to these technical functions."

In the rationale from the Dakar Board Resolution, the Board acknowledged that continuing to evolve the RAA is an important element of a program to protect registrants and safeguard the stability of a single interoperable Internet. The Board request for policy consideration of the remaining recommendations for RAA amendments that are not negotiated into the RAA is intended to produce "meaningful amendments in the global public interest with the twin goals of registrant protection and stability in mind." Accordingly, this request would be consistent with the ICANN mission to ensure the stable and secure operation of the Internet's unique identifier systems.

Whether the issue is broadly applicable to multiple situations or organizations

As the RAA is expected to apply uniformly to all registrars, the issue is broadly applicable to multiple situations or organizations. Should the policy processes initiated as a result of the Board request produce a new form of RAA, or specific new policies that are intended to become "consensus policies," these would eventually become applicable to all registrars. The timing of the effectiveness varies depending upon whether the modification is a new consensus policy that would be effective immediately, or whether the modification is not intended to produce a new consensus policy. In such cases, these might be reflected in a new form of RAA that would be effective upon renewal by the Registrar. Should a new form of RAA not be effective immediately, ICANN may consider offering incentives to registrars for early adoption.

Whether the issue is likely to have lasting value or applicability, albeit with the need for occasional updates

Because the new form of RAA to be produced out of this effort is expected to become the standard agreement that ICANN offers all new registrars and all existing registrars, it is likely to have lasting value and applicability. Similarly, any specific policies or RAA amendments that may emerge from the policy processes are also expected to have lasting value and applicability.

Whether the issue will establish a guide or framework for future decision-making

The RAA amendments or new policies emerging any policy initiative that is initiated by the GNSO Council should serve as a guide or framework for future decision-making with respect to the topics addressed.

Whether the issue implicates or affects an existing ICANN policy

Many of the Proposed Amendment Topics address existing ICANN policies. These include policies related to WHOIS, the UDRP, and general contract conditions that were either adopted through formal consensus policies, or were otherwise reflected in the current form of RAA. It is expected that these policies may be modified through the policy processes to be initiated by the GNSO Council as a result of the Board Dakar resolution.

Recommended action

Staff has confirmed that the Proposed Amendment Topics are within the scope of the ICANN policy process and the GNSO.

Under the new Annex A of the Bylaws,[27] the GNSO Council is required to commence a PDP upon instruction of the ICANN Board. As the Board has described this issue in its rationale for the Dakar RAA Resolution as a "matter of extreme urgency," Staff recommends that the GNSO Council initiate the PDP on the RAA Contractual Conditions to consider each of the Proposed Amendment Topics identified in the Final Issue Report that have not been fully addressed through the RAA negotiations. By the time of the publication of the Final Issue Report, Staff believes that there will be information available that identifies the remaining topics from the Proposed Amendment Topics that are not likely to be included in the amended RAA produced from those negotiations.

[27] Under Section 4 of the new Bylaws, the GNSO Council is required to commence a PDP at the Board's request within the timeline specified in the GNSO Council's PDP Manual. The PDP Manual specifies that if the Board requests an Issue Report, the Council shall note for the record the confirmation of receipt of the Issue Report and the formal initiation of the PDP. No vote is required for such action. The PDP Manual also specifies that the issue would be taken up at the next GNSO Council meeting following the delivery of the Final Issue Report, provided that it is delivered at least 8 days prior to the meeting.

Recommendations to Manage a PDP involving 24 Amendment Topics

Managing one PDP for all of the Proposed Amendment Topics may be overwhelming for the community volunteers and the Staff needed to complete this PDP on an expedited basis, as directed by the Dakar RAA Resolution. Staff suggests that the GNSO Council consider dividing these Proposed Amendment Topics into approximately 4 separate PDPs, to be run in parallel as follows:

- Registrar Duties, Responsibilities and Obligations RAA Amendments
- WHOIS DATA Related RAA Amendments
- RAA Amendments concerning Resellers and Privacy and Proxy Providers
- Contract Administration Related RAA Amendments

Staff is interested in soliciting comments during the Public Comment Forum on whether this proposal for structuring the PDP(s) on the RAA would be an efficient way of managing the review of a potentially unwieldy list of amendment topics.

XII. Conclusion and Next Steps

A Final Issue Report will be published following the closing of the Public Comment Forum on this Preliminary Issue Report. After the delivery of the Final Issue Report, the GNSO Council is required under the Bylaws to initiate the PDP.

Given the breadth and scope of RAA amendment topics under consideration, the GNSO Council is encouraged to take the time before the publication of the Final Issue Report to review its current projects to determine whether any should be suspended while the RAA related PDP(s) are underway. Staff believes that the policy effort to support consideration of these Proposed Amendment Topics will be considerable, requiring significant time and resources from the GNSO community as well as from Staff.

Annex 1 - Board Resolution

Registrar Accreditation Agreement Amendments

Whereas the GNSO Council resolved on 4 March 2009 to support Registrar Accreditation Agreements (RAA) amendments as documented in http://gnso.icann.org/drafts/current-list-proposed-raa-amendments-16dec08.pdf, recommend to the Board that they be adopted, and to form a Drafting Team to discuss further amendments to the RAA and to identify those on which further action may be desirable.

Whereas the Council provided a report from that working group that prioritized recommendations for RAA amendment topics.

Whereas law enforcement representatives have met on several occasions to develop and deliver recommendations for Registrar Accreditation Agreement amendment topics and those recommendations have been endorsed by ICANN's Governmental Advisory Committee.

Whereas the GNSO has extensively debated the process for developing and approving amendments to the RAA.

Whereas continuing to evolve the RAA is an important element in a program to protect registrants and safeguard the stability of a single interoperable Internet.

Whereas the gTLD registrars and ICANN are entering into negotiations to consider existing recommendations and deliver a proposed set of meaningful amendments in the global public interest with the twin goals of registrant protection and stability in mind.

Resolved (2011.10.28.31), the ICANN Board directs negotiations to commence immediately, resulting in proposed amendments to be provided for consideration at ICANN's meeting in Costa Rica in March 2012.

Resolved, (2011.10.28.32), the subject of the negotiations should include law enforcement and GNSO working group recommendations as well as other topics that would advance the twin goals of registrant protection and DNS stability.

Resolved (2011.10.28.33), the Board also requests the creation of an Issue Report to undertake a GNSO policy development process (PDP) as quickly as possible to address remaining items suited for a PDP.

Rationale for Resolutions 2011.10.28.31 – 2011.10.28.33

> *The Board wishes to convey its sense of urgency on this issue. Law enforcement agencies and a GNSO working group have developed a list of specific recommendations for amending the RAA to provide greater protections for registrants and reduce abuses. Yet no action has been taken on these recommendations. The Board requires action. Direct negotiations between the contracted parties is seen as a way to rapidly develop a set of amendments for consideration.*
>
> *For the benefit of the ICANN community, the Board is also requesting an issues report to explore the Policy alternatives for developing and making binding changes to the RAA. The Board also recognizes and accepts the GAC Communiqué statement that the ICANN Board to take the necessary steps to ensure that ICANN's multi-stakeholder process effectively addresses these GAC-endorsed proposals as a matter of extreme urgency.*
>
> *This resolution will have no fiscal impact, nor will it have any impact on the security, stability and resiliency of the domain name system.*

ANNEX 2 List of Proposed Amendment Topics

Summary of Proposed Amendment Topics

A. Registrar Obligations/Duties

A.1 Malicious conduct – registrar duty to investigate

A.1.a Prohibition of certain illegal, criminal or malicious conduct

A.1.b Registrar obligations to collect, securely maintain and validate data

A.2 Designation and publication of technically competent point of contact on malicious conduct issues available 24/7 basis

A.3 Require greater disclosure of registrar contact information, information on form of business organization, officers, etc.

A.4 Require greater disclosure of registrar affiliates/multiple accreditations

A.5 Prohibition on registrar cybersquatting

A.6 Clarification of registrar responsibilities in connection with UDRP proceedings

A.7 Require registrars to report data breaches

A.8 Registrar responsibilities for acts of affiliates

A.9 Staff to draft registrar code of conduct if registrars fail to do so by certain time

B. Privacy & Proxy Services/Resellers

B.1 Obligations of privacy/proxy services made available in connection with registration re data escrow; Relay function; Reveal function

B.2 Registrar responsibility for cancellation under appropriate circumstances of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal

B.3 Define “reseller” and clarify registrar responsibility for reseller compliance

B.4 Registrar disclosure of privacy/proxy services made available in connection with registration; and responsibility of registrar compliance by such services

B.5 Registrars to disclose resellers and vice-versa

C. WHOIS Data

C.1 Require PCI compliance in registration process
C.2 Service Level Agreement on Whois availability
C.3 Define circumstances under which registrar is required to cancel registration for false Whois data and set reasonable time
C.4 Spell out "verification" process registrars are required to undertake after receiving report of false Whois data
C.5 Require links to Whois Data Problem Reporting System on Whois results pages and on registrar home page

D. Contract Administration

D.1 Expand scope of authority to terminate accreditation
D.2 Streamline arbitration process in cases of dis-accreditation
D.3 Streamline process of adding new gTLDs to accreditation

Key: "LEA" – Law Enforcement Agencies
"RAA DT" – Refers to the RAA Drafting Team which compiled the Final Report on improvements to the RAA

Note: The term "eligible for consensus policy development" is also sometimes referred as "within the picket fence"

A. REGISTRAR OBLIGATIONS/DUTIES/RESPONSIBILITIES

A.1	**Malicious Conduct – Registrar Duty To Investigate**	**Priority Designation in RAA Final Report: High**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Sections 4.2.1; 4.26	**<u>LEA</u>**: Registrars should provide complainants with a well-defined, auditable way to track abuse complaints (e.g. a ticketing or similar tracking system) **<u>RAA DT</u>** 1) Incorporate a provision in the RAA establishing a duty of registrars to investigate and report to ICANN on actions the registrar has taken in response to reports received from a credible third-party demonstrating illegal malicious conduct involving domain names 2) Adopt a Registrar Code of Conduct (RAA 3.7.1) that incorporates provisions to achieve similar results	**Draft Registrar Code of Conduct:** 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. 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.

A.1.a	Prohibition of Certain Illegal, Criminal or Malicious Conduct (Based on Section 5.3.2.1)
	Recommendations/Options **DRAFT REGISTRAR CODE OF CONDUCT** 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.

A.1.b	**Registrar obligations to collect, securely maintain and validate data**
Options	**Recommendations/Options**
Eligible for consensus policy development RAA Sections 4.2.1; 4.26	**LEA:** 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. 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) Cross validate the phone number area code with the provided address and credit card billing address

A.2	Designation and publication of technically competent point of contact on malicious conduct issues, available on 24/7 basis	
		Priority Designation in RAA Final Report: High
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.1	**LEA:** 1) 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. 2) 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. **RAA DT** 1) Registrars must be required to prominently post their abuse desk contact information. 2) Include a new RAA Section 3.12.7 requiring resellers to provide and maintain complete and accurate contact information for a	**Draft Registrar Code of Conduct:** 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. **GNSO RAA Motion:** 1) ICANN-accredited registrars must provide to ICANN staff, and ICANN staff must keep on record, a valid physical address for the purpose of receiving legal service. This record must include a valid street address, city, appropriate region, telephone number and fax number. Registrars must publish this information on their respective web sites, and must notify ICANN staff and update their published addresses within 30 days of a change of address 2) ICANN-accredited registrars must provide to ICANN staff, and ICANN staff must keep on record, the names of

	point of contact for malicious conduct, including allegations of fraud and domain name abuse (e.g., recommended by SSAC 38).	each registrar's respective corporate President, Vice President, and Secretary, or the appropriate equivalents of those positions. These data may be made available upon request to a verified representative of a law enforcement agency, in a manner agreed to by ICANN staff, ICANN-accredited registrars, and representatives of law enforcement agencies. Registrars will notify ICANN of any changes in this information within 30 days of a change. 3) ICANN-accredited registrars must publish on their respective web sites e-mail and postal mail addresses to which law enforcement actions may be directed. The e-mail address will use a uniform convention (example: lawenforcement@example.tld <mailto:lawenforcement@example.tld>) to facilitate ease of use by law enforcement agencies. Registrars may, at their individual discretion, include language in this section of their web sites, directed to the general public, that makes clear the use and expected outcomes of these points of contact and identifies the appropriate points of contact for other forms of business. Requests submitted by verified law enforcement agencies to this discrete point of contact must receive an acknowledgement of receipt from the registrar within 24 hours. 4) Law enforcement agencies provide, within six months of the date of approval of this policy by the ICANN Board and via the general advice of the GAC to the Board, their recommendations for a database and identification system that allows for expedient identification to a registrar of a law enforcement agency, and verification of the contacting party as a law enforcement agency upon that agency's first contact with a registrar.

A.3	Require greater disclosure of registrar contact information, information on form of business organization, officers, etc.	
		Priority Designation in RAA Final Report: High
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.1	**LEA:** 1) 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. 2) Registrar should be legal entity within the country of operation, and should provide ICANN with official certification of business registration or license. 3) 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 **RAA DT** 1) Registrars to provide to ICANN (and keep current) their operational and office locations, full address, phone and fax numbers, for posting on the Internic website, and to post the	**Draft Registrar Code of Conduct:** **1) 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. **2) 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

	same information on their own website 2) Registrars to specify to ICANN their form of business organization, jurisdiction under which organized, and agent for service of legal process, and to keep this information current	executive management structure, as well as any changes in the controlling ownership of Registrar. **3) 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. **4) 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.
A.4	**Require greater disclosure of registrar affiliates/multiple accreditations**	**Priority Designation in RAA Final Report: High**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.1	**<u>LEA:</u>** 1) ICANN should require all registrars, registries, proxy services, resellers and all third party beneficiaries of any contracts, policies of ICANN to publicly display ownership, parent companies, subsidiaries and business associations. 2) Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests. **<u>RAA DT:</u>** 1) Insert a new section in the RAA requiring registrars to submit, on an annual basis, additional information to ICANN, for use in	**Draft Registrar Code of Conduct:** Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests.]

	vetting and verifying the identity of the registrar and its affiliates. Such categories of information could include: additional details on the registrar's officers and directors (e.g., names, postal addresses and contact information); names, postal addresses and contact information of affiliated entities that engage in domain related services; the identity and ownership of registrar's parent corporations, if applicable; names, postal addresses and contact information for significant resellers (e.g. resellers registering more than 50,000 or 5% of its domain names under management); and names, postal addresses and contact information for any privacy/proxy services offered or made available by registrar or its affiliates. 2) Registrars to specify to ICANN any parent, subsidiary, affiliate, or entity under common control which is also an accredited registrar, and to keep this information current.	

A.5	Prohibition on registrar cybersquatting	Priority Designation in RAA Final Report: High
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.5	**RAA DT:** 1) Incorporate terms in the RAA that explicitly prohibit cybersquatting 2) Currently, the violation of RAA Section 3.7.2 entitled "applicable laws and government regulations" by registrars is a breach of the RAA. Under section 5.3.4 a registrar has fifteen working days after ICANN gives notice of a breach to cure. A violation of RAA Section 3.7.2 is the type of offense that should result in immediate termination of the RAA. Therefore, insert in RAA Section 5.3.2 the right to immediately terminate the RAA when a registrar violates RAA Section 3.7.2 or the prohibition against cybersquatting. 3) Adopt a Registrar Code of Conduct (RAA 3.7.1) that incorporates provisions to achieve similar results. 4) Amend RAA to require Registrar to provide ICANN with list of pending litigation or claims alleging cybersquatting. 5) Termination of accreditation	

A.6	Clarification of registrar responsibilities in connection with UDRP proceedings	Priority Designation in RAA Final Report: High
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.3	**RAA DT:** Establishment of firm and enforceable deadlines for registrars (a) to respond to dispute resolution provider's requests for information in connection with registrar verification processes at the inception of a UDRP proceeding; and (b) to provide for transfer of the domain name to the petitioner pursuant to standard and (preferably) simplified processes.	

A.7	**Require registrars to report data breaches**	**Priority Designation in RAA Final Report: Medium**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.1	**RAA DT:** 1) Insert language in the RAA defining a security breach as "the unauthorized access to or disclosure of registrant account data". 2) Insert language in the RAA requiring a registrar to promptly disclose, to ICANN and affected registrants, any security breach of registrar's IT network affecting its domain management systems after the discovery or notification of a security breach. 3) Insert language in the RAA defining promptly disclose by the registrar as "action taken in the most expedient timeframe possible and without unreasonable delay". Action(s) taken by a registrar should be consistent with the legitimate needs of law enforcement, as applicable, or any other measures a registrar determines are necessary to define the scope of the breach and restore the reasonable integrity of the data system.	

A.8	**Registrar responsibilities for acts of affiliates**	**Priority Designation in RAA Final Report: Medium**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.1	**RAA DT:** Registrar A should be subject to sanctions under RAA for directing or assisting registrar B (under common control) in serious violations	

A.9 Staff to draft registrar code of conduct if registrars fail to do so by time certain Priority Designation in RAA Final Report: Medium		
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.1	**RAA DT:** 1) Establish a Code and require registrar compliance 2) If a Registrar Code of Practice is developed, some issues for possible inclusion: • Requirement on registrars to cancel a registration if inaccurate or unreliable WHOIS information is not corrected • Prominently display contact information. ICANN SAC also recently advised that Registrars should have a 24/7 contact number that connects to a person technically able to deal with abuse notification • Use commercially available verification systems to provide time of registration validations • Prohibitions (or stronger prohibitions) on front running, cyber squatting • Have stronger action by registrars on breaches by resellers	

B. PRIVACY & PROXY SERVICES/RESELLERS

B.1 Obligations of privacy/proxy services made available in connection with registration re data escrow; Relay function; Reveal function Priority Designation in RAA Final Report: High		
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section 4.2.6	**LEA:** 1) 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. 2) Require registrars to collect and preserve contact data for beneficial registrant/licensee even when registration is channeled through proxy or privacy service made available in connection with the registration process. **RAA DT:** 1) Insert provisions in the RAA that require a registrar and its resellers to escrow privacy or proxy registration data, and at a minimum, disclose the points of contact for privacy or proxy service providers and a description of the privacy or proxy services offered to their customers. 2) Develop and implement the program in RAA Section 3.12.4 of the RAA giving ICANN the ability to establish or "make available a program granting recognition to resellers that escrow privacy or proxy registration data". Create a similar contractual provision in RAA Section 3.4.1 for registrars. 3) Explicit requirement for all proxy and private registration services to escrow contact data on beneficial registrant/licensee. 4) Conspicuous Notice • "display a conspicuous notice to such customers at the time an	**Draft Registrar Code of Conduct:** 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.

	election is made to utilize such privacy or proxy service that their data is not being escrowed." -- eliminate this clause 5) Insert in RAA Section 3.7.7.3 provisions that require privacy or proxy services to forward allegations of malicious conduct, cybersquatting, and other illegal activities to privacy or proxy service customers. 6) Develop contract language and/or advisories that clarify the language of RAA Section 3.7.7.3, including the definition of "reasonable evidence of actionable harm" with input from registrars and non-contracted parties. 7) The GNSO could discuss what forms of illegal malicious conduct and what standard of evidence should result in a requirement to reveal the contact information of customers of privacy or proxy services, consistent with procedures designed to respect any applicable protections for privacy and freedom of expression. 8) Specify circumstances under which proxy registration services are required to disclose actual contact data of beneficial registrants/licensees, and apply the same standards to private registration services. 9) Amend the language in RAA Section 3.7.7.3 as follows: "A Registered Name Holder licensing use of a Registered Name accepts liability for harm caused by wrongful use of the Registered Name, unless it promptly (i.e. within five business days) discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm."	

B.2	**Registrar responsibility for cancellation under appropriate circumstances of registrations made by other privacy/proxy services for noncompliance with Relay and Reveal**	**Priority Designation in RAA Final Report: High**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**LEA:** If proxy/privacy registrations are allowed, registrars are to accept proxy/privacy registrations only from ICANN accredited Proxy Registration Services. ICANN to implement accreditation system for Proxy Services using the same stringent checks and assurances as provided in these points, to ensure that all proxy services used are traceable and can supply correct details of registrant to relevant authorities. **RAA DT:** 1) ICANN to accredit all proxy or privacy registration services, and registrars prohibited from accepting registrations from unaccredited services 2) Make registrars responsible for compliance with all RAA obligations by providers of proxy or private registration services that are made available in connection with the registrar's registration process. 3) Amend the language in RAA Section 3.7.7.3 as follows: "A Registered Name Holder licensing use of a Registered Name accepts liability for harm caused by wrongful use of the Registered Name, unless it promptly (i.e. within five business days) discloses the current contact information provided by the licensee and the identity of the licensee to a party providing the Registered Name Holder reasonable evidence of actionable harm."	**Draft Registrar Code of Conduct:** 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.3 Define “reseller” and clarify registrar responsibility for reseller compliance		
Options Eligible for Consensus Policy Development RAA Section: 4.2.1	**Recommendations/Options** **LEA:** 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. **RAA DT:** Require registrars to guarantee reseller compliance with RAA and indemnify ICANN for breaches by resellers that are not remediated within a reasonable time.	**Additional Information**

B.4 Registrar disclosure of privacy/proxy services made available in connection with registration; and responsibility of registrar for compliance by such services		Priority Designation in RAA Final Report: High
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**RAA DT:** Require registrars on an annual basis to provide a list of privacy or proxy registration services, including points of contact for privacy or proxy service providers and a description of the services provided or made available by a registrar to its customers. This information could be provided either directly to ICANN or published by a registrar on its web site. This requirement would assist ICANN in determining compliance with RAA Section 3.4.1 related to escrow of Whois information.	
B.5 Registrars to disclose resellers and vice versa		**Priority Designation in RAA Final Report: High**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.1	**RAA DT:** 1) Require registrars to disclose all authorized resellers to ICANN and to the public 2) Require resellers to disclose to all registrants the identity and contact information of the registrar sponsoring a particular registration	

C. WHOIS DATA

C.1	**Require PCI compliance in registration process**	**Priority Designation in RAA Final Report: High**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**LEA:** 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). Each registrar is required to validate the following data upon receipt from a registrant: (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	

	RAA DT Registrars are to be required to avail themselves of commercially available identity verification systems that will provide for time-of-registration validations.	
C.2 Service Level Agreement on Whois availability		**Priority Designation in RAA Final Report: Medium**
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**LEA:** ICANN should require Registrars to have a Service Level Agreement for their Port 43 servers. **RAA -DT** 1) SLA on WHOIS Availability 2) It certainly seems reasonable to me that the RAA contain an SLA provision re WHOIS, just like the registry contracts do.	**Draft Registrar Code of Conduct:** 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.

C.3	Define circumstances under which registrar is required to cancel registration for false Whois data and set reasonable time limits for registrar action Priority Designation in RAA Final Report: High	
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**RAA -DT:** 1) Require registrars to terminate registrations of registrants who violate RAA provisions relating to disclosure of accurate contact information in appropriate circumstances. 2) Clarify the existing registrar obligation to take reasonable steps to verify or correct Whois data in response to reported inaccuracies. At a minimum, "reasonable steps" to investigate a reported inaccuracy should include promptly transmitting to the registrant the "inquiries" concerning the accuracy of the data that are suggested by RAA Subsection 3.7.7.2. The inquiries should be conducted by any commercially practicable means available to the registrar: by telephone, e-mail, or postal mail. A registrar should also report to ICANN what action, if any, was taken in response to the reported inaccuracy. If the registrant has materially breached the registration agreement (by either failing to respond to registrar's inquiries or by willfully providing inaccurate information), then the registrar should either suspend or delete the domain registration. 3) Adopt a Registrar Code of Conduct (RAA 3.7.1) that incorporates provisions to achieve similar results. 4) WDPRS • Require registrars to cancel a registration if inaccurate or unreliable WHOIS information is not corrected	

C.4 Spell out “verification” process registrars are required to undertake after receiving report of false Whois data **Priority Designation in RAA Final Report: Medium**		
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**<u>RAA DT:</u>** Adopt a Registrar Code of Conduct (RAA 3.7.1) that incorporates provisions to achieve similar results.	

C.5 Require links to Whois Data Problem Reporting System on Whois results pages and on registrar home page **Priority Designation in RAA Final Report: Medium**		
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.6	**<u>RAA DT:</u>** Registrar’s Whois service must include with query results a link or referral to the Whois Data Problem Reporting System or its successor on Internic page	

D. CONTACT ADMINISTRATION

D.1 Expand scope of authority to terminate accreditation		Priority Designation in RAA Final Report: Medium
Options	**Recommendations/Options**	**Additional Information**
Eligible for Consensus Policy Development RAA Section: 4.2.1; 4.2.8	**LEA:** 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…" **RAA -DT** 1) Incorporate two provisions in RAA Section 5.3 that establish ICANN's right to immediately terminate the RAA when a Registrar either: (1) abandons or ceases to conduct business as a registrar; or (2) repeatedly and willfully has been in fundamental and material breach of its obligations at least three times within any twelve month period. 2) Insert a new RAA Section 5.3.8 as follows: "Registrar repeatedly and willfully has been in fundamental and material breach of its obligations at least three times within any twelve month period." 3) Three Times is an excessive threshold • "or (ii) Registrar shall have been repeatedly and willfully in fundamental and material breach of its obligations at least three (3) times within any twelve (12) month period." 4) Clause 5.3.2.1 is at the mercy of lengthy appeals processes which place the registrant community at risk while legal dramas unfold – intermediate measures are required. 5) The Draft Registrar Disqualification Procedure contains language that potentially could be incorporated into the RAA	

	at section 5.3.	
D.2 Streamline arbitration process in cases of dis-accreditation		**Priority Designation in RAA Final Report: Medium**
Options Eligible for GNSO Consideration RAA Section: 5.4	**Recommendations/Options** **RAA DT:** 1) Insert the following language in RAA Section 5.6: “There shall be one arbitrator agreed by the parties from a list of AAA arbitrators, or if the parties cannot agree within fifteen calendar days of the AAA request that the parties designate an arbitrator, the AAA shall choose and appoint an arbitrator, paying due regard to the arbitrator’s knowledge relating to the domain name system. 2) Amend the RAA to allow ICANN to terminate or suspend a registrar's accreditation if a stay has not been ordered within ten business days after the filing of the arbitration.	**Additional Information**

D.3 Streamline process of adding new gTLDs to accreditation		Priority Designation in RAA Final Report: Medium
Options	**Recommendations/Options**	**Additional Information**
Eligible for GNSO Consideration RAA Section: 5.4	**RAA DT:** 1) The trademark related license terms could be incorporated as a separate section within the body of the RAA, eliminating the need for a separate appendix. 2) ICANN can create an electronic process that allows Registrars in good standing (i.e., not subject to an outstanding breach notice) to request the right to carry additional gTLDS, and ICANN will electronically submit the names to the registries of those registrars authorized by ICANN to carry their TLD. Any additional terms and conditions necessary for the TLD can be incorporated into the terms of the Registry-Registrar Agreement	

Excerpts of relevant RAA Provisions

4.2 Topics for New and Revised Specifications and Policies. New and revised specifications and policies may be established on the following topics:

4.2.1 issues for which uniform or coordinated resolution is reasonably necessary to facilitate interoperability, technical reliability, and/or operational stability of Registrar Services, Registry Services, the DNS, or the Internet;

4.2.2 registrar policies reasonably necessary to implement ICANN policies or specifications relating to a DNS registry or to Registry Services;

4.2.3 resolution of disputes concerning the registration of Registered Names (as opposed to the use of such domain names), including where the policies take into account use of the domain names;

4.2.4 principles for allocation of Registered Names (e.g., first-come/first-served, timely renewal, holding period after expiration);

4.2.5 prohibitions on warehousing of or speculation in domain names by registries or registrars;

4.2.6 maintenance of and access to accurate and up-to-date contact information regarding Registered Names and nameservers;

4.2.7 reservation of Registered Names that may not be registered initially or that may not be renewed due to reasons reasonably related to (a) avoidance of confusion among or misleading of users, (b) intellectual property, or (c) the technical management of the DNS or the Internet (e.g., "example.com" and names with single-letter/digit labels);

4.2.8 procedures to avoid disruptions of registration due to suspension or termination of operations by a registry operator or a registrar, including allocation of responsibility among continuing registrars of the Registered Names sponsored in a TLD by a registrar losing accreditation; and

4.2.9 the transfer of registration data upon a change in registrar sponsoring one or more Registered Names.

5.4 Term of Agreement; Renewal; Right to Substitute Updated Agreement. This Agreement shall be effective on the Effective Date and shall have an initial term running until the Expiration Date, unless sooner terminated. Thereafter, if Registrar seeks to continue its accreditation, it may apply for renewed accreditation, and shall be entitled to renewal provided it meets the ICANN-adopted specification or policy on accreditation criteria then in effect, is in compliance with its obligations under this Agreement, as it may be amended, and agrees to be bound by terms and conditions of the then-current Registrar accreditation agreement (which may differ from those of this Agreement) that ICANN adopts in accordance with Subsection 2.3 and Subsection 4.3. In connection with renewed accreditation, Registrar shall confirm its assent to the terms and conditions of the then-current Registrar accreditation agreement by signing that accreditation agreement. In the event that, during the Term of this Agreement, ICANN posts on its web site an updated form of registrar accreditation agreement applicable to Accredited registrars, Registrar (provided it has not received (1) a notice of breach that it has not cured or (2) a notice of termination of this Agreement under Subsection 5.3 above) may elect, by giving ICANN written notice, to enter an agreement in the updated form in place of this Agreement. In the event of such election, Registrar and ICANN shall promptly sign a new accreditation agreement that contains the provisions of the updated form posted on the web site, with the length of the term of the substituted agreement as stated in the updated form posted on the web site, calculated as if it commenced on the date this Agreement was made, and this Agreement will be deemed terminated.

ANNEX 3 GNSO Council Motion on Certain Law Enforcement Recommendations

Motion carried on 6 October 2011

Motion regarding the nature of Internet-based criminal activity and the information and tools available to help address crime that involves the domain name system

WHEREAS, the Registrar Stakeholder Group has consulted extensively with representatives of international law enforcement agencies regarding the nature of Internet-based criminal activity and the information and tools available to help address crime that involves the domain name system; and

WHEREAS, the Registrar Stakeholder Group has reviewed law enforcement proposals and requests regarding registrar cooperation in addressing online crime; and

RESOLVED, the GNSO Council requests an Issues Report on the following possible policy revisions and/or additions:

1. ICANN-accredited registrars must provide to ICANN staff, and ICANN staff must keep on record, a valid physical address for the purpose of receiving legal service. This record must include a valid street address, city, appropriate region, telephone number and fax number.
2. Registrars must publish this information on their respective web sites, and must notify ICANN staff and update their published addresses within 30 days of a change of address.
3. ICANN-accredited registrars must provide to ICANN staff, and ICANN staff must keep on record, the names of each registrar's respective corporate President, Vice President, and Secretary, or the appropriate equivalents of those positions. These data may be made available upon request to a verified representative of a law enforcement agency, in a manner agreed to by ICANN staff, ICANN-accredited registrars, and representatives of law enforcement agencies. Registrars will notify ICANN of any changes in this information within 30 days of a change.
4. ICANN-accredited registrars must publish on their respective web sites e-mail and postal mail addresses to which law enforcement actions may be directed. The e-mail address will use a uniform convention (example: lawenforcement@example.tld) to facilitate ease of use by law enforcement agencies. Registrars may, at their individual discretion, include language in this section of their web sites, directed to the general public, that makes clear the use and expected outcomes of these points of contact and

identifies the appropriate points of contact for other forms of business. Requests submitted by verified law enforcement agencies to this discrete point of contact must receive an acknowledgement of receipt from the registrar within 24 hours.

5. Law enforcement agencies provide, within six months of the date of approval of this policy by the ICANN Board and via the general advice of the GAC to the Board, their recommendations for a database and identification system that allows for expedient identification to a registrar of a law enforcement agency, and verification of the contacting party as a law enforcement agency upon that agency's first contact with a registrar.

5. The Issue Report should include a freedom-of-expression impact analysis.