

## ICANN Board-GAC Consultation: Law Enforcement Due Diligence Recommendations—Due Diligence and Registrar Accreditation Agreement

### EXPLANATION OF ISSUE/HISTORY

The Registrar Accreditation Agreement (RAA) was last updated in 2009 in an effort to improve protections for registrants, provide additional compliance tools and bring the agreement into line with the current market practices. At that time, the Board directed Staff to follow a specific process, including negotiations with registrars, public consultations, and public comment periods, to arrive at changes to the RAA. That effort led to a new draft RAA which was presented to the GNSO for approval in late 2008 (per the procedure specified in the RAA). Many in the GNSO and the ALAC stated the proposed amendments did not go far enough. A revised RAA was unanimously approved by the GNSO Council in Mexico City in 2009 on the condition that further work would be undertaken through a joint ALAC/GNSO effort to (i) draft a registrant rights charter, (ii) identify additional amendment topics, and (iii) propose next steps for producing a new RAA to be adopted by ICANN.

The GNSO Final Report<sup>1</sup> was published prior to Cartagena and describes a list of possible amendment topics for the RAA, as well as suggested approaches for conducting negotiations to produce a new form of the RAA. The Final Report includes a list of 12 topics designated as “high priority amendments” and a list of 10 topics designated as “medium priority” topics. These high/medium priority topics include several topics reflecting ICANN compliance concerns<sup>2</sup> as well as those addressed in the LE recommendations. The Final Report also documents the divergent views regarding the next steps for producing the new form of RAA, with “Process A” (open negotiations between the Registrars/ICANN and selected third party observers) receiving strong support in the drafting team, and the minority position “Process B” (closed negotiations only among registrars and ICANN) receiving support only from registrars. The GNSO Council is expected to vote on the procedure for producing the new form RAA, including the format of the negotiations (whether open/closed to parties other than Staff and the Registrars).

In the meantime, members of the law enforcement (“LE”) community put forward proposals designed to aid in the prevention and disruption of efforts to exploit domain registration

---

<sup>1</sup> The Final Report on Proposals for Improvements to the RAA is posted at <http://gns0.icann.org/correspondence/rap-idt-to-gns0-council-15nov10-en.pdf>

<sup>2</sup> For more information on Staff compliance concerns and input to the RAA drafting team, see: <http://forum.icann.org/lists/gns0-aa-dt/msg00106.html> and <http://forum.icann.org/lists/gns0-aa-b/msg00123.html>

procedures by criminal groups for criminal purposes.<sup>3</sup> These proposals address two broad areas- enhanced due diligence to be conducted by ICANN on Registrars, and proposals for amending the Registrar Accreditation Agreement. These law enforcement proposals have received support from a number of agencies globally, including the U.K. Serious Organized Crimes Agency, the U.S. Federal Bureau of Investigation, and the Canadian Royal Mounted Police.

The LE RAA proposals received support from the GAC. In its communiqué during the Nairobi meeting (the “Nairobi Communiqué”), the GAC noted that the law enforcement proposals were favorably viewed by the high tech crime experts in the G8 and Interpol. The Nairobi Communiqué further stated that it hoped that the RAA Working Group would examine the proposals from law enforcement and take them into consideration during their work on the amendments. As described above, the RAA Working Group devoted significant time to evaluating the LE RAA proposals. The LE recommendations have been endorsed by the GAC in its Brussels Communiqué, but no specifics have been provided regarding how these proposals could be incorporated into the New gTLD Program, or more broadly to be applicable to existing gTLDs.

## **REMAINING AREAS OF DIFFERENCE**

The main difference between the GAC and ICANN positions appears to be the timing. Both the GAC and ICANN have the same goals: to implement the LE recommendations in order to provide a safer, more stable environment for users. To the extent possible, some are embedded in the new gTLD process in a form where the obligations suggested in the LE recommendations for registrars are being applied to registries. Other recommendations are not applicable to registries; some though can be passed through to registrars as described elsewhere.

The difference in timing is related to the expectations of the consideration and adoption of the LE recommendations. There is a sense among the community that ICANN can cause the recommendations to be adopted immediately into the New gTLD Program or for existing TLDs.

Presently, ICANN is working within the construct of the ICANN’s policy processes and GNSO Council’s work related to the RAA. The process for new or existing TLDs is essentially the same. ICANN’s is supporting the GNSO Council’s process to produce an RAA that would apply to both existing and new gTLDs, and expects that many law enforcement recommendations would be addressed in that manner. Since the first new gTLDs will not be delegated until 2012 at the earliest, it is reasonable to plan that this work will be completed before then.

---

<sup>3</sup> The law enforcement proposals are included in their entirety as Annex G to the Final Report on Proposals for Improvements to the RAA dated 18 October 2010 <http://gns0.icann.org/issues/raa/raa-improvements-proposal-final-report-18oct10-en.pdf>.

Another reason for the difference in expected timing between the GAC and ICANN positions lies in whether the LE recommendations are more appropriately addressed through the GNSO Council's policy development processes rather than through directly negotiated contract amendments. To the extent that the above-mentioned recommendations reflect a new or significantly different approach (such as the proxy/privacy or WHOIS validation recommendations), ICANN would view those recommendations as something that should be addressed as a new policy initiative under the GNSO Council's mandate rather than through contract negotiations.

## RELEVANT GUIDEBOOK SECTIONS OR OTHER PAPERS

ICANN supports law enforcement efforts for enhanced due diligence and registrar obligations. The key challenge for ICANN is identifying the appropriate process and timeline for implementing such changes<sup>4</sup>:

- Recommendations affecting only ICANN, such as an internal ICANN process, can be considered and acted upon quickly.
- Recommendations requiring a change of existing policy or creation of a new policy, are for ICANN's multi-stakeholder Supporting Organizations and Advisory Committees, such as the GNSO and GAC, to follow its policy development processes as outlined in the Bylaws.
- Recommendations affecting existing contractual relationships, such as the RAA, must follow the process outlined in the agreement.
- Recommendations specific to the new gTLD program may be addressed through changes to the Applicant Guidebook.

The law enforcement recommendations are not specific to the New GTLD Program but are intended to apply more broadly to all gTLDs, new and old, although some concepts have been incorporated in the New gTLD Program. Some of the recommendations for gTLD registrars are also good ideas for gTLD registries. They have been adapted and applied to gTLD registries through the New gTLD program either through heightened requirements in the application process or changes to the registry agreement. The chart attached as **Annex A** summarizes the law enforcement recommendations, and their treatment or proposed treatment by ICANN.

For example, the due diligence related recommendations are viewed as affecting only ICANN, thereby allowing ICANN to consider and act upon them quickly. Therefore, in response to the law enforcement recommendations, ICANN initiated a process last year to revamp its processes to accredit new registrars. In November 2010,<sup>5</sup> ICANN published its proposal for public

---

<sup>4</sup> The appropriate process is suggested in Appendix A, which describes actions being taken in the new gTLD program and also by the GNSO.

<sup>5</sup> For details on the new accreditation process proposed by ICANN, please refer to: <http://www.icann.org/en/announcements/announcement-2-22nov10-en.htm>

comment on its proposed changes to enhance ICANN's Registrar accreditation evaluation process. The law enforcement recommendations were evaluated and considered by ICANN in developing its proposal. The published proposal includes terms and conditions for applicants, as well as adoption of a new Accreditation Application Form designed to hold applicants responsible for providing accurate information to ICANN.<sup>6</sup> In addition, ICANN announced that it will conduct additional due diligence checks and sought public comment on whether these should include criminal records, financial history and solvency, and corporate/company structure and ownership. Upon closing of the public comment in January 2011, ICANN plans to revise the process as appropriate in response to comments raised, and implement the new process as expeditiously as possible.

With regard to the proposed LE amendments to the RAA, ICANN has supported GNSO Council work, and plans to address the law enforcement proposals during the negotiation process that is to follow the GNSO Council vote - expected at the next GNSO meeting. To date, ICANN has not taken steps to incorporate the LE amendment proposals into the New gTLD program, preferring instead to allow the GNSO Council (who have the law enforcement recommendations in hand) to produce a new RAA that would apply to both new and existing gTLDs. ICANN is open to designating a member of the law enforcement community to be designated as an observer in that process.

In the event the GNSO Council discussion does not result in timely or firm recommendations, ICANN could explore other avenues for implementing additional law enforcement recommendations, including:

- Separate new RAA – Negotiations that consider law enforcement and GNSO recommendations can start at any time.
- New gTLD Registry Agreement – New registry obligations that are being incorporated into the new Registry Agreement can, in some cases, flow down to create registrar additional requirements.
- Registrar Code of Conduct- Under the current RAA (Section 3.7.7) applicable to all Registrars, Registrars are required to abide by a Code of Conduct that ICANN adopts which is supported by a consensus of ICANN accredited registrars. ICANN could commence the process to develop a Code of Conduct with the registrars.
- Voluntary Adoption of a new RAA. Similar to the approach taken by ICANN for the 2009 Form RAA, ICANN could provide incentives to registrars adopting the new form Agreement once a new RAA is created.

Under any of the above scenarios, ICANN will consult with the registrars and the broad ICANN community to properly analyze and vet the impact of any of these additional requirements on users, contracted parties and the DNS. This consultation will begin immediately upon the upcoming conclusion of the current policy effort.

**ANNEX A**

The chart below summarizes the current status of the law enforcement recommendations, the proposed treatment by the joint GNSO/ALAC RAA Drafting Team (DT), and adoption in the New gTLD Program. Although not all items have been prioritized by the DT, ICANN could still adopt or negotiate them during the next phase of negotiations. Some are viewed as out of scope for the New gTLD Program, but may be addressed through other processes, such as policy development or contract negotiations. Other recommendations intended for registrars have been applied to registries as part of the New gTLD Program.

	<b>Law Enforcement Recommendation</b>
1	<p><i>Proxy Related Recommendations</i></p> <p><i>The RAA should not explicitly condone or encourage the use of Proxy Registrations or Privacy Services</i></p> <p><b>New gTLD Program:</b> Does not explicitly condone or encourage use of proxy/privacy services or mention proxy/privacy registrations.  <b>GNSO RAA Final Report:</b> Not prioritized by the DT</p>
	<p><i>Registrars are to accept proxy/privacy registrations only from ICANN accredited Proxy Registration Services;</i></p> <p><b>New gTLD Program:</b> Out of scope of the new gTLD Program, since it is a policy issue.  <b>GNSO RAA Final Report:</b> Not prioritized by the DT</p>
1.b	<p><i>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.</i></p> <p><b>New gTLD Program:</b> Out of scope of the new gTLD Program. To the extent this changes the existing RAA, it is a policy discussion.  <b>GNSO RAA Final Report:</b> DT prioritized some similar approaches to proxy/privacy services</p>
2	<p><i>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...”</i></p> <p><b>New gTLD Program:</b> Out of scope of the new gTLD Program, but applicants are subject to background checks that include certain criminal behavior and instances of domain name abuse.  <b>GNSO RAA Final Report:</b> Not prioritized by the DT</p>

3	<p><i>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.</i></p> <p><b>New gTLD Program:</b> Aspects adopted for applicants  <b>GNSO RAA Final Report:</b> Similar approach prioritized by the DT</p>
4	<p><i>Registrars must publicly display of the name of CEO, President, and/or other responsible officer(s).</i></p> <p><b>New gTLD Program:</b> Out of scope for the New gTLD Program but officers are subject to background checks.  <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
5	<p><i>Registrars with multiple accreditations must disclose and publicly display on their website parent ownership or corporate relationship, i.e., identify controlling interests.</i></p> <p><b>New gTLD Program:</b> Aspects adopted for applicants  <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
6	<p><i>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 (or similar) filing; d. change of ownership; e. criminal convictions ; f. legal/civil actions</i></p> <p><b>New gTLD Program:</b> Registry Agreement includes change of control and criminal conviction terms applicable to registries  <b>GNSO RAA Final Report:</b> Not prioritized by the DT</p>
7	<p><i>Registrar should be legal entity within the country of operation, and should provide ICANN with official certification of business registration or license.</i></p> <p><b>New gTLD Program:</b> Some aspects included for applicants who must furnish proof of permission to operate.  <b>GNSO RAA Final Report:</b> Not prioritized by the DT</p>

8	<p><i>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.</i></p> <p><b>New gTLD Program:</b> Out-of-scope <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
9	<p><i>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.</i></p> <p><b>New gTLD Program:</b> Out-of-scope <b>GNSO RAA Final Report:</b> DT prioritized alternative approach (require PCI compliance in the registration process)</p>
10	<p><i>Each registrar is required to validate the following data upon receipt from a registrant: (1) Technical Data(a) IP addresses used to register domain names.(b) E-mail Address (i) Verify that registration e-mail address(es) are valid.(2) Billing Data(a) Validate billing data based on the payment card industry (PCI standards), at a minimum, the latest version of the PCI Data Security Standard (DSS).(3) Contact Data(a) Validate data is being provided by a human by using some anti-automatic form submission technology (such as dynamic imaging) to ensure registrations are done by humans.(b) Validate current address WHOIS data and correlate with in-house fraudulent data for domain contact information and registrant's IP address.(4) Phone Numbers(i) Confirm that point of contact phone numbers are valid using an automated system. (ii) (ii) Cross validate the phone number area code with the provided address and credit card billing address.</i></p> <p><b>New gTLD Program:</b> Out-of-scope, there is no privity of contract between the registrant and the registry. <b>GNSO RAA Final Report:</b> DT prioritized different approach (require PCI compliance in the registration process)</p>



11	<p><i>Registrar must provide abuse contact information, including the SSAC SAC 038 recommendations below:</i></p>
	<ul style="list-style-type: none"> <li>· <i>Registrars must prominently publish abuse contact information on their website and WHOIS.</i></li> </ul> <p><b>New gTLD Program:</b> Included similar approach for Registries  <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
	<ol style="list-style-type: none"> <li>1. <i>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., <a href="http://www.&lt;registar&gt;.&lt;TLD&gt;/abuse.html">http://www.&lt;registar&gt;.&lt;TLD&gt;/abuse.html</a>.</i></li> </ol> <p><b>New gTLD Program:</b> Out-of-scope  <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
	<ol style="list-style-type: none"> <li>2. <i>Registrars should provide ICANN with their abuse contact information and ICANN should publish this information at <a href="http://www.internic.net/regist.html">http://www.internic.net/regist.html</a>.</i></li> </ol> <p><b>New gTLD Program:</b> Some aspects included for registries in Registry Agreement (registries to provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for malicious conduct inquiries, and must provide ICANN notice of any changes)  <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
	<p><i>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.</i></p> <p><b>New gTLD Program:</b> Some aspects included for registries  <b>GNSO RAA Final Report:</b> DT prioritized similar approach</p>
	<p><i>Registrars should provide complainants with a well-defined, auditable way to track abuse complaints (e.g., a ticketing or similar tracking system).</i></p> <p><b>New gTLD Program:</b> Out of scope  <b>GNSO RAA Final Report:</b> Not prioritized by DT</p>

12	<p><i>ICANN should require Registrars to have a Service Level Agreement for their Port 43 servers.</i></p> <p><b>New gTLD Program:</b> SLA included for Thick WHOIS published by Registry <b>GNSO RAA Final Report:</b> Prioritized by the DT</p>
----	---