Registries Stakeholder Group Statement Regarding the "Registration Abuse Policies Working Group Initial Report"
26 March 2010

The comments below are submitted on behalf of the gTLD Registries Stakeholder Group (RySG) regarding the "Registration Abuse Policies Working Group Initial Report" of 12 February 2010. The comments that follow represent a consensus position of the RySG as further detailed at the end of the document.

The RySG commends the RAPWG for the hard work done by its volunteer members, who approached a number of challenging issues and achieved consensus on several of them.

Scope Issues, and Definitions of "Registration" and "Use" (*RAPWG Report Section 4.2*)

ICANN contracts authorize the development of Consensus Policies on topics where uniform or coordinated resolution is reasonably necessary to facilitate the interoperability, technical reliability, or operational stability of registrars, registries, the DNS, or the Internet. After a year of work and examining an exhaustive list of issues brought forward by members from diverse constituencies, the RAPWG did not present any issue that might be construed as requiring uniform or coordinated resolution reasonably necessary to facilitate the interoperability, Security and/or Stability of the Internet or DNS. We do not see where or how the basic security or stability of the DNS has been compromised by any of the registration abuses discussed in the report. Nor have we seen how the Security and Stability of the registry database for the TLD, or, functional and performance specifications for the provision of Registry Services (as defined in registry contracts as being subject to Consensus Policies) have been invoked.

The RAPWG discussed the new Expedited Registry Security Request (ERSR), which offers a flexible mechanism for registries to receive contractual variances from ICANN in order to respond to significant malicious threats to the DNS itself or a TLD's operations. The ERSR helps address a problem within ICANN's remit -- how to be prepared for and deal with threats to the basic Stability and Security of the DNS itself. The ERSR might obviate the need for some policy-making in that area.

While e-crime is a recognized problem that impacts many parties, we believe that Registry Services, the DNS, and the Internet overall continue to function in a stable and reliable manner. While e-crime is a real and sophisticated problem, it is not ICANN's mission to concern itself with everything that happens on the Internet or via the DNS. It is essential for ICANN to restrict its activities to its limited technical coordination mission.

We agree that making distinctions between *registration* issues and domain *use* issues are very important. They provide one test for whether a particular activity is within or outside of GNSO and ICANN policy-making scope. Careful consideration of these issues and limiting of scope are consistent with ICANN's limited mission.

In the Issues Report, "staff and the General Counsel's office" considered the issue, and stated:

> "4.2.3 of the RAA between ICANN and accredited registrars provides for the establishment of new and revised consensus policies concerning the registration of

> domain names, including abuse in the registration of names, **but policies involving the use of a domain name (unrelated to its registration) are outside the scope of policies that ICANN could enforce on registries and/or registrars. The use of domain names may be taken into account when establishing or changing registration policies. Thus, potential changes to existing contractual provisions related to abuse in the registration of names would be within scope of GNSO policy making. Consideration of new policies related to the use of a domain name unrelated to its registration would not be within scope."** [Emphasis added. Page 41: http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf]

It is important to note that domain name uses unrelated to registration issues are largely outside the scope of policy-making. This is consistent with ICANN's mission and mandate. As a fundamental principle, ICANN has historically and rightfully avoided examining or regulating content or speech (good or bad). And ICANN has never taken upon itself to regulate the social or technical uses of the DNS and the Internet unless they are proven to threaten the very stability and security of the DNS system itself. As per its bylaws, ICANN should always be "respecting the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission requiring or significantly benefiting from global coordination."

We agree that the RAPWG took a rational course "by determining what registration issue exists (if any), and considering if or how it has any inherent relation to a domain name or registration process." And it correctly said that "Other questions that should be considered in evaluating potential abuses and related policies are if and how any policy decision might impact the use of domain names, and establishing whether and to what extent the use of domain names affects the stability and security of the DNS itself, and if so how." The GNSO should continue to emphasize fact-based policy-making processes, and carefully examine the impact of policy on affected parties.

RAPWG Report Section 5.1: Cybersquatting

The RySG **supports** the first recommendation:
"The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues Report to investigate the current state of the UDRP, and consider revisions to address cybersquatting if appropriate. This effort should consider:

- ***How the UDRP has addressed the problem of cybersquatting to date, and any insufficiencies/inequalities associated with the process.***
- ***Whether the definition of cybersquatting inherent within the existing UDRP language needs to be reviewed or updated."***

The URDP is the long-standing mechanism for addressing cybersquatting, and has been largely successful. We note that the above recommendation is about the UDRP *only*, and not other post-domain-creation rights protections mechanisms (RPMs). Discussion of other RPMs should be specifically excluded from the charter of any GNSO effort that results from the above recommendation. The RAPWG drafted a second recommendation about other RPMs in an effort to keep the two issues separate.

The GNSO should make policy decisions regarding cybersquatting based on facts and data. Scale issues have not been quantified adequately for the GNSO, and an adequate factual basis for policy-making has not been provided via other efforts such as the IRT.

We strongly **reject** the second RAPWG cybersquatting recommendation, for *"**the initiation of a Policy Development Process by requesting an Issues Report to investigate the appropriateness and effectiveness of how any Rights Protection Mechanisms that are developed elsewhere in the community (e.g. the New gTLD program) can be applied to the problem of cybersquatting in the current gTLD space.**"* The RAPWG was split on this recommendation, with the support coming from intellectual property protection advocates.

It is inadvisable to even begin considering the imposition of those evolving rights protection mechanisms in the existing TLDs for the following reasons:

- Those proposed rights-protection mechanisms upend several long-established legal principles. One is that the registrant is the party responsible for ensuring he or she is not infringing upon the rights of others. Another is that rights holders have the responsibility for protecting their own intellectual property. Unilaterally shifting responsibility, cost, or liability from registrants and rights holders to ICANN-contracted parties is unfair and unjustified.
- The proposals for those RPMs continue to evolve, and it is unclear what they might involve.
- The effectiveness of those proposed mechanisms is hypothetical. It is unknown if they can deliver the cost and process benefits their advocates promised or asked for.
- It is unknown what impacts or unintended consequences they may have for registrants, for speech and expression, etc.
- Some parties have called for imposition of the trademark clearinghouse RPM during ongoing registry operations, which could effectively stop real-time, first-come registrations. This would be a major change to the industry, with wide-ranging repercussions for registrants and the costs they pay for gTLD domain names; it could place gTLDs at a disadvantage relative to ccTLDs, and other problems.

RAPWG Report Section 5.3: Gripe Sites; Deceptive, and/or Offensive Domain Names

We support the majority position of the RAPWG. Our reasoning is:

- ICANN is not a good forum to make recommendations regarding moral standards.
- "Potential harm to consumers" is a vague standard.
- The recommendation is problematic for global TLDs, and it was a matter closed in .COM/.NET/.ORG many years ago.
- The community has more pressing issues to address.

RAPWG Report Section 5.4: Fake Renewal Notices

We believe that this may be an issue with resellers. In any case, registrars are responsible for the registration activities performed by their resellers.

RAPWG Report Section 6.7.3: Malicious Uses of Domain Names

The RySG supports the RAPWG's recommendation for ***"the creation of non-binding best practices to help registrars and registries address the illicit use of domain names."***

We support it because these practices will lead to real benefits for many parties across the Internet, because responsible parties should pay attention to the issue of e-crime, and because ICANN is a natural place for registries and registrars to come together in a bottom-up fashion to share ideas and experiences in this area.

We note that this effort is for non-binding best practices. E-crime research shows conclusively that different registries face different issues regarding the criminal use of domain names -- and some face no problems at all. One-size-fits-all solutions are therefore not applicable or effective. Non-binding best practices are appropriate because registries can adapt them according to their varying needs.

The RySG feels that non-binding best practices will not only be helpful and make a positive impact, but they will also avoid some insuperable issues. Allowing registries (and registrars) to make a difference by choice is practical and generally effective. ICANN-contracted parties have—and should continue to have—the ability to set relevant terms of service for their respective TLDs or registrar service. Private parties who are willing to take action against illegal activity within their own networks or realms should be free to appropriately craft their own contracts, terms of service, and solutions as conditions suggest. Software companies, ISPs, hosting providers, network operators, Web site and online service providers, intellectual property owners, other businesses, and individual computer users all have the right to regulate harmful behavior in their realms, and we do not believe that contracted parties should be treated differently in this respect. Problems with phishing, malware, etc. are resolved in this way every day without involving ICANN, and we believe that most solutions to deal with e-crime should not involve ICANN intervention. We note that one of ICANN's core values, enshrined in its bylaws, is: "To the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties."

It is true that some registrars do a poor job of responding to abuse reports. But there are hundreds of ICANN-accredited registrars, of all sizes and business models, and some will always be under-resourced or vulnerable. This is a systemic problem that goes hand-in-hand with a competitive domain name market, and forcing registries to compensate is not the solution. We do suggest that ICANN focus efforts on registrars who do not comply with their contractual obligations.

The RySG feels that key issues concerning the illicit or criminal use of domain names are outside of ICANN's purview, and beyond the scope of GNSO policy-making. ICANN's ability to regulate uses of domain names unrelated to registration issues is very limited. And it is not possible for ICANN to force contracted parties to mitigate criminal uses of the DNS.

1. Making policy to mitigate criminal uses of domain names is not reasonably and appropriately related to ICANN's technical coordination function. Again, it is not ICANN's mission to concern itself with everything that happens on the Internet or via the DNS. ICANN is not a venue for legislating or coordinating crime-fighting, or for enforcing civil law. It is not within ICANN's purview to place gTLD registries in a position to become extensions of law enforcement regimes around the world, by requiring registries to take action against a domain name that may be in

violation of one or more nation's laws. ICANN cannot be a substitute for or compensate for the roles of law enforcement and governments.

2. In the ICANN context, combating everyday e-crime is mainly a matter of identifying and disabling some (not all) domain names that are being used for illegal purposes. To require registries to act against illicitly used domain names will expose registries to unknown liabilities, and it is unclear whether ICANN has an effective ability to effectively protect contracting parties from those liabilities. The RAPWG Initial Report identifies some of the thorny issues surrounding intent, risk, and indemnification, and how registries could be legally exposed. Most e-crime issues do not have any relation to domain name registration issues within GNSO and ICANN policy-making scope.

3. ICANN is not practically suited to creating or overseeing detailed policies and procedures in such a rapidly evolving environment as cybercrime, where the criminals and responders are continually employing new measures and counter-measures. Instead, it is more helpful to let private actors have the freedom and power to act within relevant legal and contractual contexts. ICANN is ill-situated to make determinations of intent and legality. And it is not within ICANN's purview to determine (or license another body to determine) which domain names are being used for illegal purposes.

4. Unfortunately, e-crime is a fact of life and will never be eliminated, and much e-crime is not directly related to domain names and domain registration processes. This is not to say that responsible parties should not get involved, or that efforts to fight e-crime are fruitless. We merely note that it is appropriate for ICANN to focus within its mission, and to explain that narrow role to its constituents and the wider public.

RAPWG Report Section 7.3: WHOIS Access

The RySG supports the two recommendations.

RAPWG Report Section 8: Uniformity of Contracts

The GNSO Council should be highly skeptical of the proposed PDP, which states that "***The RAPWG recommends the creation of an Issues 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.***"

That proposal is unjustified because it would pursue an undefined problem, it may be a pretext to pursue some unstated goals, and it could unwisely harm a variety of parties. The RySG opposes the idea, and urges the GNSO Council to reject it.

The PDP recommendation is a process or solution in search of a problem. The GNSO Council asked the RAPWG to "Understand if registration abuses are occurring that might be curtailed or better addressed if consistent registration abuse policies were established." In other words, to look for specific problems that might need to be solved with specific policies. But instead, some RAPWG members have voted for this PDP, which is a recommendation for the GNSO to pursue unbounded policy-making to solve undefined problems. Despite ample opportunity, those advocates have not explained what problem(s) this approach might solve, or why it is needed. Nor did they fulfil their obligation under the RAPWG Charter to explain how existing registration abuse provisions are generally ineffective in addressing registration abuse. PDPs should not be "fishing trips."

The Consensus Policy process should be used to craft specific policies to address specific problems that require a uniform approach across registries and registrars. *The Consensus Policy process is the mechanism specifically designed to create uniformity where it is needed, and it guarantees uniformity.* If there is a registration abuse that needs attention, the GNSO can make Consensus Policy about that abuse, and the resulting policy will be applied to all contracted parties.

The PDP advocates on the RAPWG sub-team on Uniformity of Contracts (the "PDP Advocates") supported the exploration of "general language with broad powers to act against all kinds of abuse," and provisions "that can anticipate future or unknown abuses." We disagree, because:

a) Policies should have stated, legitimate purposes.
b) Those ideas are impractical, because it is difficult if not impossible to anticipate future or unknown abuses.
c) Those ideas are undesirable, because they do not include adequate consideration of who is being harmed, how, and to what extent. The RAPWG's membership agreed unanimously that "The party or parties harmed, and the substance or severity of the abuse, should be identified and discussed in relation to a specific proposed abuse"-- but the PDP advocates did not address this requirement. General and/or pre-emptive policies may create collateral damage and harm registrants or other parties in unknown and unexpected fashions. In those cases where ICANN has already defined a registration abuse policy, the abuse definitions and the policies have been clearly and consistently expressed, and this should continue to be the case.

Further, uniformity for the sake of uniformity does not always solve a policy problem. In fact, some amount of non-uniformity in registry contracts may be necessary or useful. For example, sTLDs currently have language in their contracts to define their unique sponsorship and eligibility needs, and resulting compliance requirements. ICANN and/or the registries might need such in the future.

We are concerned that "uniformity of contracts" is a cloaked initiative to deny contracted parties their existing rights to set their own terms of service. Registries must retain their existing rights to establish operational standards, policies, procedures, and practices for their registries in a non-arbitrary manner and applicable to all registrars, and consistent with ICANN's standards and policies. This right is consistent with ICANN's core values, which include: "depending on market mechanisms to promote and sustain a competitive environment"; "delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties"; and "respecting the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission requiring or significantly benefiting from global coordination."

The PDP Advocates that did the Uniformity of Contracts analysis did not always distinguish adequately between *registration abuse* provisions and provisions designed to address *malicious uses* of domains. This distinction can be critical for policy-making, as explained in detail in the RAPWG's report.

Some who recommend the PDP may also be interested in "uniformity of contracts" as a way to require contracted parties (or one contracted party) to mitigate malicious uses of domain names. When discussing the concept of "uniformity of contracts," one RAPWG member has referred several times to a lack of a provision in the .COM/.NET contract that other registries have relied upon to create policies to fight phishing, malware, and other malicious uses of domain names.[1] Such participants may believe that once a domain name is registered, almost anything about or related to that domain name--including its technical or social uses--can be regulated by ICANN, and pushed down to contracted parties to enforce. This approach ignores the boundaries of GNSO and ICANN policy-making, and is improper.

If the goal of the "uniformity of contracts" PDP recommendation is really to change a particular contract, or to force registries to suspend domain names, then such goals should be made explicit for the GNSO and the community.

GNSO gTLD Registries Stakeholder Statement of Support

Issue: **"Registration Abuse Policy Working Group Initial Report"**

A supermajority of 11 RySG members supported this statement.

General RySG Information

- Total # of eligible RySG Members[2]: 14
- Total # of RySG Members: 13
- Total # of Active RySG Members[3]: 13
- Minimum requirement for supermajority of Active Members: 9
- Minimum requirement for majority of Active Members: 7
- # of Members that participated in this process: 13
- Names of Members that participated in this process:

[1] http://forum.icann.org/lists/gnso-rap-dt/msg00185.html and http://forum.icann.org/lists/gnso-rap-dt/msg00547.html and http://forum.icann.org/lists/gnso-rap-dt/msg00585.html and http://forum.icann.org/lists/gnso-rap-dt/msg00602.html

[2] All top-level domain sponsors or registry operators that have agreements with ICANN to provide Registry Services in support of one or more gTLDs are eligible for membership upon the "effective date" set forth in the operator's or sponsor's agreement (RySG Articles of Operation, Article III, Membership, ¶ 1). The RySG Articles of Operation can be found at <http://gnso.icann.org/files/gnso/en/improvements/registries-sg-proposed-charter-30jul09-en.pdf>. The Universal Postal Union recently concluded the .POST agreement with ICANN, but as of this writing the UPU has not applied for RySG membership.

[3] Per the RySG Articles of Operation, Article III, Membership, ¶ 6: Members shall be classified as "Active" or "Inactive". A member shall be classified as "Active" unless it is classified as "Inactive" pursuant to the provisions of this paragraph. Members become Inactive by failing to participate in a RySG meeting or voting process for a total of three consecutive meetings or voting processes or both. An Inactive member shall have all rights and duties of membership other than being counted as present or absent in the determination of a quorum. An Inactive member may resume Active status at any time by participating in a RySG meeting or by voting.

1. Afilias (.info and .mobi)
2. DotAsia Organisation (.asia)
3. DotCooperation (.coop)
4. Employ Media (.jobs)
5. Fundació puntCAT (.cat)
6. Museum Domain Management Association – MuseDoma (.museum)
7. NeuStar (.biz)
8. Public Interest Registry (.org)
9. RegistryPro (.pro)
10. Societe Internationale de Telecommunication Aeronautiques – SITA (.aero)
11. Telnic (.tel)
12. The Travel Partnership Corporation – TTPC (.travel)
13. VeriSign (.com, .name & .net)

- Names & email addresses for points of contact:
  - Chair: David Maher, dmaher@pir.org
  - Alternate Chair: Jeff Neuman, Jeff.Neuman@Neustar.us
  - Secretariat: Cherie Stubbs, Cherstubbs@aol.com

Regarding the issue noted above, the level of support in the RySG is summarized below.

1. **Level of Support of Active Members**: Supermajority

   1.1. # of Members in Favor: 11

   1.2. # of Members Opposed: 0

   1.3. # of Members that Abstained: 0

   1.4. # of Members that did not vote: 2

2. **Minority Position**(s): N/A