

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

Registration Abuse Policies Working Group

Initial Report

Submitted [TBC]

[ROUGH DRAFT: IN PROCESS.]
Version: 2 February 2010

- 1/2/10 13:14
Deleted: 27 January

STATUS OF THIS DOCUMENT

This is the Initial Report of the Registration Abuse Policies Working Group (RAPWG), prepared by ICANN staff for submission to the GNSO Council on [TBC] and posted for public comment. A Final Report will be prepared following the closure of the public comment period.

27 **1. Table of Contents**

28 **1. TABLE OF CONTENTS2**

29 **2. EXECUTIVE SUMMARY.....3**

30 **3. BACKGROUND, PROCESS, AND NEXT STEPS4**

31 **4. DISCUSSION OF CHARTER AND SCOPE QUESTIONS7**

32 **5. POTENTIAL REGISTRATION ABUSES EXPLORED13**

33 **6. MALICIOUS USE OF DOMAIN NAMES31**

34 **7. WHOIS ACCESS53**

35 **8. UNIFORMITY OF CONTRACTS63**

36 **9. META-ISSUES.....78**

37 **10. CONCLUSIONS, RECOMMENDATIONS, & NEXT STEPS84**

38 **ANNEX I – WORKING GROUP CHARTER85**

39 **ANNEX II - THE WORKING GROUP AND ATTENDANCE88**

40
41

Marika Konings 2/2/10 11:25
Deleted: 1 . TABLE OF CONTENTS . 2 .

41 **2. Executive Summary**

42

43 ▪ TBC

44

44 3. Background, Process, and Next Steps

45

46 3.1 Background

47

48 ▪ On 25 September 2008, the GNSO Council adopted a motion requesting an issues report
49 on registration abuse provisions in registry-registrar agreements. The issues report was
50 submitted to the GNSO Council on 29 October 2008 and provides an overview of
51 existing provisions in registry-registrar agreements relating to abuse and includes a
52 number of recommended next steps, namely for the GNSO Council to:

53 - **Review and Evaluate Findings**

54 A first step would be for the GNSO Council to review and evaluate these findings,
55 taking into account that this report provides an overview of registration abuse
56 provisions, but does not analyse how these provisions are implemented in practice
57 and whether they are deemed effective in addressing registration abuse.

58 - **Identify specific policy issues**

59 Following the review and evaluation of the findings, the GNSO Council would need
60 to determine whether there are specific policy issues regarding registration abuse.
61 As part of this determination it would be helpful to define the specific type(s) of
62 abuse of concern, especially distinguishing between registration abuse and other
63 types of abuse if relevant.

64 - **Need for further research**

65 As part of the previous two steps, ICANN Staff would recommend that the GNSO
66 Council determines where further research may be needed – e.g. is lack of
67 uniformity a substantial problem, how effective are current registration abuse
68 provisions in addressing abuse in practice, is an initial review or analysis of the
69 UDRP required?’

70 ▪ The GNSO Council voted on 18 December to form a drafting team to create a proposed
71 charter for a working group charged with investigating the open issues identified in

72 Registration Abuse Policies report. The drafting team was formed and met for the first
73 time on 9 January 2009. They finalized a charter (see Annex I), which was adopted by
74 the GNSO Council on 19 February 2009, for a Registration Abuse Policies Working Group
75 (RAPWG). The GNSO Council will not make a decision on whether or not to initiate a
76 Policy Development Process (PDP) on registration abuse policies until the RAPWG has
77 presented its findings.

78

79 3.2 Process

80

81 ▪ The RAPWG started with discussing and developing a working definition of abuse, which
82 has served as a basis to further explore the scope and definition of registration abuse.

83 ▪ The RAPWG has been researching and discussing what “registration abuse” is, including:

- 1/2/10 14:48
Deleted: '

84 a. How ‘registration’ is defined. This term was not explicitly defined, and is essential
85 for understanding the “registration” versus “use” issues that the charter and Issues
86 Report call attention to.

87 b. Which “aspects of the subject of registration abuse are within ICANN’s mission to
88 address and which are within the set of topics on which ICANN may establish
89 policies that are binding on gTLD registry operators and ICANN-accredited
90 registrars.” As part of the RAPWG research, a presentation was provided by ICANN
91 staff about policy-making scope issues and past PDPs.

92 ▪ The RAPWG developed a list of potential abuses. The RAPWG discussed each of these
93 proposed abuses, sometimes facilitated by the creation of sub-teams. The RAPWG
94 developed a definition for each, considered whether they are abusive or not,
95 determined if and how registration issues are implicated in them and whether
96 regulation is within or outside of policy-making scope, and developed recommendations
97 for further consideration. Further details can be found in the following chapter of this
98 report.

99 ▪ Several sub-tams were formed [throughout this process to explore more complicated](#)
100 [abuse types and other Registration Abuse topics identified in the charter.](#) Sub-teams

Marika Konings 2/2/10 11:14
Deleted: to specifically
Marika Konings 2/2/10 11:15
Deleted: deep dive on abuse types and
Marika Konings 2/2/10 11:15
Deleted: RAP topics. Such s

101 [focused on](#); [Cybersquatting](#), [Name Spinning](#), [Malware/Botnet](#), [Phishing/Malware and](#)
102 [Uniformity of Contracts](#), [Findings and recommendations that resulted from these efforts](#)
103 [can be found in the chapters below](#).

105 3.3 Next Steps

- 107 ■ Even though the RAPWG is not a Policy Development Process (PDP) Working Group, in
108 the interest of transparency and participation it decided to follow the practice of PDP
109 Working Groups by producing an Initial Report for community comment and
110 consideration before finalizing the report and its recommendations for submission to
111 the GNSO Council. The RAPWG will review the comments received and issue a Final
112 Report following the closing of the public comment period.

113

Marika Konings 2/2/10 11:15

Deleted: were

Marika Konings 2/2/10 11:16

Deleted: , Front-Running, etc

Marika Konings 2/2/10 11:16

Deleted: The Uniformity of Contracts sub-team was formed in order to research whether registration abuses are occurring that might be curtailed or better addressed if consistent policies / contract language were established, The findings and recommendations that resulted from this effort can be found in the "uniformity of Contracts" chapter.

- 1/2/10 13:28

Deleted: ,

113 4. Discussion of Charter and Scope Questions

114

115 4.1 Abuse definition

116

117 The RAPWG developed a consensus definition of abuse, which served as a basis to further
118 explore the scope and definition of registration abuse. This definition reads:

- 1/2/10 14:45

Deleted: working

119 *Abuse is an action that:*

- 1/2/10 14:45

Deleted: working

120 a. *Causes actual and substantial harm, or is a material predicate of such harm, and*

121 b. *Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a*
122 *stated legitimate purpose, if such purpose is disclosed.*

123

124 Note:

125 * The party or parties harmed, and the substance or severity of the abuse, should be
126 identified and discussed in relation to a specific proposed abuse.

127 * The term "harm" is not intended to shield a party from fair market competition.

128 * A predicate is a related action or enabler. There must be a clear link between the predicate
129 and the abuse, and justification enough to address the abuse by addressing the predicate
130 (enabling action).

131 * The above definition of abuse is indebted to the definition of "misuse" in the document
132 "Working Definitions for Key Terms that May be Used in Future WHOIS Studies" prepared by
133 the GNSO Drafting Team¹.

134

¹ 18 February 2009, at ¹ 18 February 2009, at <http://gnso.icann.org/issues/whois/whois-working-definitions-study-terms-18feb09.pdf>

135 **4.2 Definitions of “registration” and “Use”**

136

137 *Registration issues* are related to the core domain name-related activities performed by
138 registrars and registries. These generally include but are not limited to:

- 139
- 140 • the allocation of registered names, and reserved names
 - 141 • maintenance of and access to accurate and up-to-date information concerning
142 domain name registrations – i.e. WHOIS information.
 - 143 • the transfer, deletion, and reallocation of domain names.
 - 144 • functional and performance specifications for the provision of Registry Services.
 - 145 • The resolution of disputes regarding whether particular parties may register or
146 maintain registration of particular domain names.

146

147 These are generally within the scope of GNSO policy-making. Many of the above are specifically
148 listed in registration agreements as being subject to Consensus Policies, and the extant
149 Consensus Policies have to do with these kinds of topics. Other potential outcomes of policy
150 work are also possible, such as advice to ICANN on possible contract amendments, or the
151 development of non-binding options such as codes of conduct or best practices.

152

153 *Registration abuses* are therefore abuses associated with the above kinds of activities or topics.
154 ICANN has made consensus policies for several registration-related abuses. Examples² include:

- 155
- 156 • The AGP Limits Policy, instituted to curb abuse of the Add Grace Period—specifically the
157 practice known as domain tasting.
 - 158 • The WHOIS Data Reminder Policy, instituted to remind registrants that provision of false
159 WHOIS information is abusive and can be grounds for cancellation of their domain name
160 registration.
 - 161 • The Inter-Registrar Transfer Policy, designed to guarantee that registrants can transfer
162 names to the registrar of their choice, and to provide standardized requirements for the
proper handling of transfer requests by registrars and registries.

² <http://www.icann.org/en/general/consensus-policies.htm>

163

164 Note that in this context, “registration” is not a synonym for the *creation* of a domain name. As
165 per the lists above, registration abuses may occur at various points in a domain name’s lifecycle.
166 The RAPWG therefore found that making distinctions between pre-domain-creation, domain-
167 creation, and post-creation abuses is sometimes not applicable or useful when considering
168 whether an abuse is in-scope for policy-making.

169

170 In contrast, domain name *use issues* concern what a registrant *does* with his or her domain
171 name after the domain is created—the purpose the registrant puts the domain to, and/or the
172 services that the registrant operates on it. These use issues are often independent of or do not
173 involve any registration issues.

174

175 A domain name can have nearly infinite uses. It can be used for various technical services, such
176 as e-mail, a Web site, file transfers, and can support subdomains. And it can support all kinds of
177 practical uses or purposes – speech and expression, e-commerce, social networking, education,
178 entertainment, and so on. Some uses of domain names are generally agreed to be abusive or
179 even criminal—such as phishing and malware distribution, which perpetrate theft and fraud.
180 Other uses – such as adult pornography or political criticism – may be considered abusive or
181 illegal in some jurisdictions but not generally. Domain names in sponsored TLDs may by design
182 be restricted to certain uses or users.

183

184 Are uses of domain names subject to GNSO policy-making? In the Issues Report that led to the
185 RAPWG, ICANN’s General Counsel wrote: “Is the issue in scope of GNSO Policy Making? Section
186 4.2.3 of the RAA between ICANN and accredited registrars *provides for the establishment of new
187 and revised consensus policies concerning the registration of domain names, including abuse in
188 the registration of names, but policies involving the use of a domain name (unrelated to its
189 registration) are outside the scope of policies that ICANN could enforce on registries and/or
190 registrars. The use of domain names may be taken into account when establishing or changing
191 registration policies. Thus, potential changes to existing contractual provisions related to abuse
192 in the registration of names would be within scope of GNSO policy making. Consideration of new*

193 *policies related to the use of a domain name unrelated to its registration would not be within*
194 *scope.”*^{3,4} [Emphasis added].

195 Other sections of the RAA and Registry Agreements may enable the GNSO to develop consensus
196 policies on the topic of registration abuse. For example, Section 4.2.1 of the RAA (as well as
197 analogous sections of various registry agreements) authorizes development of consensus
198 policies on topics where the uniform or coordinated resolution is reasonably necessary to
199 facilitate the interoperability, technical reliability, or operational stability of registrars, registries,
200 the DNS, or the Internet.⁵ The Registry Agreements generally limit Consensus Policy-making to
201 core registration issues.⁶

202

203 Careful consideration of these issues and limiting of scope seems to be consistent with ICANN’s
204 mission. In its 2002 “Working Paper on ICANN Mission and Core Values,” the Committee on
205 ICANN Evolution and Reform commented on the registration-versus-use issue. It said “Though
206 some of ICANN’s registry-level gTLD policies are non-technical in nature, all relate directly to
207 ICANN’s mission to coordinate the assignment of unique identifiers to ensure stable functioning
208 of these systems. For example, the need for dispute resolution mechanisms in the gTLDs flows

³ “GNSO Issues Report on Registration Abuse Policies,” 29 October 2008, pages 4-5.

<http://gnso.icann.org/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf>

⁴ See also <http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm>, paragraph 4.2. The new Registrar Accreditation Agreement (RAA) notes that a Consensus Policy may be established regarding the “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.”

⁵ Please also refer to the transcript of the 1 June 2009 RAP meeting, describing the presentation by Margie Milam on the scope of Consensus policies related to the topic of registration abuse, posted at <http://gnso.icann.org/calendar/index.html#june>

⁶ Principles for allocation of registered names, prohibitions on warehousing of or speculation in domain names, reserved names, maintenance of and access to accurate and up-to-date WHOIS information; procedures to avoid disruptions of domain name registration due to suspension or termination of operations by a registry operator or a registrar, and domain name disputes.

209 from the problem of unique assignment: it is the assigned domain name string itself that is at
210 issue.... [RAPWG note: i.e. a registration issue is involved.] By contrast, disputes over the content
211 of an e-mail message, ftp file, or web page bear no inherent relation to the assigned domain
212 name, and therefore fall outside the scope of ICANN's policy-making scope. ICANN therefore
213 does not base its policies on the content served by websites, contained in e-mail messages, or
214 otherwise accessed by domain names.”⁷ ICANN’s Core Values⁸ also state that ICANN should
215 respect the innovation and flow of information made possible by the Internet by limiting
216 ICANN's activities to those matters within ICANN's mission, and “To the extent feasible and
217 appropriate, delegating coordination functions to or recognizing the policy role of other
218 responsible entities that reflect the interests of affected parties”—perhaps such as courts, law
219 enforcement, and contracted parties.

220

221 Members of the RAPWG devoted significant discussion to the differences between registration
222 issues and use issues and how they may intersect. The RAPWG also found that the distinctions
223 can provide logical boundaries for policy-making. For example, some members noted that
224 ICANN is not in a position to create policies affecting speech or what kinds of e-commerce
225 should be allowed via domain names, because those typically are uses of domain names and do
226 not implicate registration issues. Others pointed out the difficulties of addressing criminal
227 domain name use via ICANN policy and contractual compliance. (This issue is explored in
228 additional depth in this Report’s section about malicious uses of domain names.)

229

230 Understanding and differentiating between domain *registration* abuses and domain *use* abuses
231 is essential in the ICANN policy context. Failure to do so can lead to confusion:

- 232 • In 2008, the GNSO initiated a PDP to examine fast-flux hosting; the concern was that
233 fast-flux was a criminal abuse that leveraged the DNS. The Fast-Flux Working Group
234 (FFWG) learned that fast-flux is actually a technical practice with both benign and
235 malicious applications, and that most criminal fast-flux hosting did not involve any

⁷ <http://www.icann.org/en/committees/evol-reform/working-paper-mission-06may02.htm>

⁸ <http://www.icann.org/en/general/bylaws.htm#>

236 changes of registration records.⁹ The FFWG determined that fast-flux was not always an
237 abuse, and it found that illicit fast-flux was a domain use issue and did not generally
238 involve registration issues. Some constituencies and observers noted that fast-flux was
239 therefore outside of policy-making scope.¹⁰ In the end, the FFWG did not recommend
240 any new policies or any changes to existing policies.

241 • The “GNSO Issues Report on Registration Abuse Policies” was an initial look into the
242 topic of registration abuse, and did not consistently and thoroughly delineate or define
243 the registration versus use issues. It sometimes used the word “abuse” to refer to both
244 registration and use problems interchangeably. At one point the Issues Report noted
245 that “various registry operators have differing policies with respect to abusive
246 registrations” while pointing to registry policies that have nothing to do with registration
247 abuses.¹¹

248

249 The RAPWG therefore approached each proposed abuse on its list by determining what
250 registration issue exists (if any), and considering if or how it has any inherent relation to a
251 domain name or registration process. Other questions that should be considered in evaluating
252 potential abuses and related policies are if and how any policy decision might impact the use of
253 domain names, and establishing whether and to what extent the use of domain names affects
254 the stability and security of the DNS itself, and if so how.

255

⁹ The DNS rotation took place at a level below the registries and registrars, and domain and nameserver records were usually not being updated on a rapid basis or at all.

¹⁰ https://st.icann.org/data/workspaces/pdp-wg-ff/attachments/fast_flux_pdp_wg:20090807173836-0-13665/original/Fast%20Flux%20Final%20Report%20-%206%20August%202009%20-%20FINAL.pdf

¹¹ See “GNSO Issues Report on Registration Abuse Policies” Section 1.5 and Annex B. The .INFO Anti-Abuse Policy is strictly aimed at malicious *uses* of domains names, such as malware and child pornography.

255 5. Potential Registration Abuses Explored

256

257 Early in the RAPWG’s existence, members were asked to propose potential abuses for
258 examination. This was to fulfil the RAPWG Charter, which asked the RAPWG to create “an
259 illustrative categorization of known abuses” and perform research “in order to understand what
260 problems may exist in relation to registration abuse and their scope, and to fully appreciate the
261 current practices of contracted parties.” In each case, the RAPWG considered the activity by
262 applying the RAPWG’s definition of abuse, and by discussing what scope and policy issues
263 existed, especially whether registration issues were fundamentally involved. In some cases the
264 RAPWG confirmed that abuse exists, and in some cases found that abuse does not exist or is out
265 of scope for policy-making.

266

267 5.1 Cybersquatting

268

269 5.1.1 Issue / Definition

270 Cybersquatting is the deliberate and bad-faith registration or use of a name that is a registered
271 brand or mark of an unrelated entity, for the purpose of profiting (typically, though not
272 exclusively, through pay-per-click advertisements). Cybersquatting is recognized as registration
273 abuse in the ICANN community, and the UDRP was originally created to address this abuse.
274 There was consensus in the RAPWG that provisions 4(a) and 4(b) of the UDRP are a sound
275 definition of Cybersquatting.¹²

276

277 5.1.2 Background

278 As part of the RAPWG's work to catalog various types of abuse, Cybersquatting was targeted as
279 an area for further work. Developing a universal, global, and technically operable definition for
280 Cybersquatting has been challenging, particularly as the RAPWG sought to balance the needs

¹² <http://www.icann.org/en/udrp/udrp-policy-24oct99.htm>

281 and interests of all parties that can potentially be harmed by the practice. The RAPWG draws a
282 distinction between competing but potentially legitimate claims and Cybersquatting, which
283 denotes a bad-faith use of another party's mark. There was consensus in the RAPWG that
284 provisions 4(a) and 4(b) of the UDRP are a sound definition of Cybersquatting. Several attempts
285 to expand the definition beyond these by borrowing from other sources (e.g. the Anti-
286 Cybersquatting Consumer Protection Act (ACPA)) have been challenging, and consensus on how
287 to proceed ultimately broke down. There was minority interest in expanding the definition to
288 include additional elements of bad faith intent, as denoted in the ACPA (i.e., 5(v) and 5(vi)). For
289 further details, please see <https://st.icann.org/reg-abuse-wg/index.cgi?cybersquatting>.

290

291 The UDRP was specifically designed to address Cybersquatting. It is used to settle disputes
292 between parties who have competing trademark claims as well as other cases in which the
293 respondent may have no trademark claim at all or is acting in bad faith. Only disputes in which
294 “the domain name is identical or confusingly similar to a trademark or service mark in which the
295 complainant has rights” are applicable for UDRP arbitration.¹³ The ICANN Web site’s UDRP page
296 also notes: “Disputes alleged to arise from abusive registrations of domain names (for example,
297 cybersquatting) may be addressed by expedited administrative proceedings that the holder of
298 trademark rights initiates by filing a [UDRP] complaint with an approved dispute-resolution
299 service provider.”¹⁴

300

301 Notwithstanding its shortcomings, the UDRP has generally been considered a success. It has
302 been used to settle thousands of cases, and WIPO has claimed that the UDRP has been a
303 deterrent to undesirable registration behavior.¹⁵ Since it went into effect in 1999, there have
304 also been complaints about the UDRP. Some of these present policy and process issues. These
305 criticisms have included: the following:

¹³ Uniform Domain Name Dispute Resolution Policy, <http://www.icann.org/en/udrp/udrp-policy-24oct99.htm>

¹⁴ <http://www.icann.org/en/udrp/udrp.htm>

¹⁵ http://www.wipo.int/pressroom/en/html.jsp?file=/redocs/prdocs/en/2005/wipo_upd_2005_239.html

- 306 • Complainants can forum-shop in attempts to find arbitrators more likely to rule in the
307 complainant's favor.
- 308 • Complainants have the ability to re-file a complaint for the same name against the same
309 respondent – in effect re-trying the same case in hopes of achieving a different
310 outcome.
- 311 • The UDRP requires the complainant prove that the domain name “has been registered
312 and is being used in bad faith.” However, many UDRP cases have been decided without
313 the domain names having ever been used. Observers have noted that the usage
314 requirement has sometimes been ignored in the UDRP “case law” that has developed
315 over the years.
- 316 • The UDRP is too expensive and too time-consuming for some brand owners, who wish
317 to pursue large numbers of potentially infringing domain names.
- 318 • The UDRP procedures lack some safeguards that are generally available in conventional
319 legal proceedings, such as appeals.
- 320 • In a possibly related issue, ICANN apparently does not enter into contracts with its
321 Approved UDRP Providers.¹⁶ This may present a number of issues. For example, in the
322 absence of such contracts, it is unclear whether ICANN has the ability to review or
323 assure general uniformity or procedural compliance.
- 324 • One UDRP service provider, the Czech Arbitration Court, recently proposed changing
325 some of its own supplemental rules in order to create an “expedited UDRP.” Some
326 community members asked whether the proposed scheme presented substantive issues
327 that can and should only be dealt with in the main ICANN UDRP Rules.¹⁷
- 328

329 Some members of the RAPWG felt that the UDRP is a useful mechanism to counter some
330 elements of cybersquatting, but were of the opinion that: "the scale of cybersquatting is
331 overwhelming and the drain on cost and resources for brand-owners to respond in all instances
332 by using only the UDRP as a remedy is prohibitive. In addition, there is insufficient up-front

¹⁶ <http://forum.icann.org/lists/cac-prop-supp-rules/msg00004.html>

¹⁷ <http://forum.icann.org/lists/cac-prop-supp-rules/index.html>

- 1/2/10 14:51

Deleted: ¹⁶

333 protection mechanisms to prevent registrants from initially registering infringing domains which
334 are freely monetized from the date of registration, via PPC and other online advertising
335 methods, thus earning revenue for the registrant. They can then simply wait until a UDRP action
336 is commenced before they give up the domain, without penalty. The burden therefore rests
337 with the trademark owner to monitor, investigate and pursue litigation in order to provide
338 protection to Internet users. This burden often includes the registration and ongoing
339 management of large domain name portfolios, consisting mainly of unwanted domains that
340 benefit only the Registry, Registrar and ICANN parties. This approach is already a major concern
341 for trademark owners, in terms of cost and resources, with the existing level of gTLDs and
342 ccTLDs, let alone the anticipated growth of new gTLDs and IDNs."

343

344 Other members disagreed with those points, expressing the following opinions:

- 345 a) The URDP is the long-standing mechanism for addressing cybersquatting. A better
346 first step would be to establish if or where the UDRP is ineffective, and make policy
347 decisions based on facts and data. While some claim that "the scale of
348 cybersquatting is overwhelming," the scale issue was not been quantified in or for
349 the RAPWG, and an adequate factual basis was not provided by the IRT.
- 350 b) Those proposed rights-protection mechanisms upend several long-established legal
351 principles. One is that the registrant is the party responsible for ensuring he or she
352 is not infringing upon the rights of others. Another is that rights holders have the
353 responsibility for protecting their intellectual property, and that shifting
354 responsibility, cost, or liability for such to ICANN-contracted parties is unfair.
- 355 c) It is inadvisable to begin considering the imposition of those evolving rights
356 protection mechanisms in the existing TLDs, when they are so controversial over in
357 the new TLD discussion. There are many legal, business, and speech issues involved.
358 The effectiveness of those proposed mechanisms is hypothetical, it is not known
359 what impacts or unintended consequences they may have, and it is unknown if they
360 can deliver the cost and process benefits their advocates promised or asked for. It is
361 unknown what consequences those mechanisms may have for speech and
362 expression. Some parties have called for imposition of the trademark clearinghouse

363 RPM during ongoing registry operations, which might effectively stop real-time,
364 first-come registrations. This would be a major change to the industry.

365

366 5.1.3 Cybersquatting Recommendation

367

368 Recommendation #1:

369

370 The RAPWG recommends the initiation of a Policy Development Process by requesting an Issues
371 Report to investigate the current state of the UDRP, and consider revisions to
372 address cybersquatting if appropriate. This effort should consider:

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

377

378 Recommendation #2:

379

380 **View A:** The RAPWG recommends the initiation of a Policy Development Process by requesting
381 an Issues Report to investigate the appropriateness and effectiveness of how any Rights
382 Protection Mechanisms that are developed elsewhere in the community (e.g. the New new gTLD
383 program) can be applied to the problem of cybersquatting. Cybersquatting in the current gTLD
384 space.

385

386 **View B:** The initiation of such a process is premature; the effectiveness and consequences of [the](#)
387 [Rights Protection Mechanisms](#) proposed for the new TLDs is unknown. Discussion of [RPMs](#)
388 should continue via the New TLD program. Experience with them should be gained before
389 considering their appropriate relation (if any) to the existing TLD space.

390

- 1/2/10 14:56

Deleted: ;

- 1/2/10 14:54

Deleted: [VERSION 19 Jan. by Martin Sutton:]

- 1/2/10 14:54

Deleted: ..

- 1/2/10 15:00

Deleted: where

- 1/2/10 14:54

Deleted: UDRP may be insufficient to curb cybersquatting

- 1/2/10 14:54

Deleted: ;

Marika Konings 2/2/10 10:51

Deleted: -

- 1/2/10 15:01

Deleted: View B: -

- 1/2/10 14:55

Deleted: RAP WG further

- 1/2/10 14:56

Deleted: RPM

- 1/2/10 14:56

Deleted: Rights Protection Mechanisms

391 **5.2 Front-Running**

392

393 **5.2.1 Issue / Definition**

394 Front-running is when a party obtains some form of insider information regarding an Internet
395 user's preference for registering a domain name and uses this opportunity to pre-emptively
396 register that domain name. In this scenario, "insider information" is information gathered from
397 the monitoring of one or more attempts by an Internet user to check the availability of a domain
398 name.

399

400 **5.2.2 Background**

401 The definition above is taken from the SSAC paper "SAC 024: Report on Domain Name Front
402 Running."¹⁸ Specifically, the RAPWG examined these documents:

- 403 1. SAC 022, <http://www.icann.org/en/committees/security/sac022.pdf>
404 2. SAC 024,
405 https://par.icann.org/files/paris/SSACReportonDomainNameFrontRunning_24Jun08.pdf
406 3. Benjamin Edelman, [http://www.icann.org/en/compliance/edelman-frontrunning-study-](http://www.icann.org/en/compliance/edelman-frontrunning-study-16jun09-en.pdf)
407 [16jun09-en.pdf](http://www.icann.org/en/compliance/edelman-frontrunning-study-16jun09-en.pdf)

408

409 The two reports by the SSAC contain a great deal of material. The RAPWG felt that a few key
410 quotes for these documents are:

- 411 • "Checking the availability of a domain name can be a sensitive act which may disclose an
412 interest in or a value ascribed to a domain name. SSAC suggests that any such domain
413 name availability lookups should be performed with care. Our premise is that a
414 registrant may ascribe a value to a domain name; that unintended or unauthorized
415 disclosure, or disclosure of an availability check by a third party without notice may pose
416 a security risk to the would-be registrant; and that availability checks may create
417 opportunities for a party with access to availability check data to acquire a domain

¹⁸ <http://www.icann.org/en/committees/security/sac024.pdf>

418 name at the expense of the party that performed an availability check, or to the benefit
419 of the party that monitored the check." (SAC 022, page 2)

- 420 • "SSAC strongly contends that any agent who collects information about an Internet
421 user's interest in a domain name and who discloses it in a public way violates a trust
422 relationship. This violation is exacerbated when agents put themselves or third parties
423 in an advantageous market position with respect to acquiring that domain name at the
424 expense of its client." (SAC 024, page 12)
- 425 • "SSAC observes a deteriorating trust relationship between registrants and registrars and
426 urge ICANN and the community to consider the implications of continued erosion and a
427 loss of faith in the registration process." (SAC 024, page 12)

428

429 The RAPWG discussed issues such as theoretical vs. actual abuse; is domain speculation an
430 abuse; expectations of trust; what is considered insider information; the interaction with the
431 add-grace period and domain tasting; possible legitimate uses of pre-registration data; and, who
432 is harmed by front-running. Commentary regarding these topics is summarized on the RAPWG
433 wiki.¹⁹ Highlights of the discussions included:

- 434 • One well-known case of front-running is described in SAC 024. Otherwise, the RAPWG
435 was unable to reference any other confirmed cases.²⁰ The WG members therefore
436 wondered whether the practice exists or is widespread enough to merit further
437 investigation or concern.
- 438 • The RAPWG members generally considered front-running an abuse, referencing the
439 SSAC's concerns about registrant expectations and breach of trust. A member also
440 offered that in a first-come-first-served environment, efforts to gain advantage or even
441 game those processes should be considered abuse.
- 442 • A member noted that the harm is to people who are new to domains and not educated
443 about how ordering takes place.

¹⁹ https://st.icann.org/reg-abuse-wg/index.cgi?domain_front_running

²⁰ The Edelman study uncovered no additional evidence of the practice. The Edelman study's methodology has been called into question, and some members considered it inconclusive.

- 444
- The issue may involve registrars or registries only indirectly. A threat may come from
445 third parties using monitoring to examine traffic and then front-run domains, perhaps
446 even using spyware or malware. In such cases, it is unknown whether a registrar or
447 registry would even be able to detect or do something about front-running. Some
448 registrars have reportedly implemented SSL-protected search pages to help guard
449 against intercepted availability check traffic.
 - Members raised some issues regarding the definition of "insider information." For
450 example, what information can registries or registrars collect about their customers, and
451 that some uses may not be inappropriate or harmful. One member stated that traffic
452 data regarding unregistered names (e.g. NX data) is by definition not registration data,
453 while another was of the opinion that such is data that can be used to decide to register
454 domains and is therefore registration data or at worst "lack-of-registration data, which
455 is merely the negative of registration data."
 - The new Add Grace Period Limits Policy effectively killed domain tasting, and may have
456 an impact on front running. To be a profitable practice, front-running might require the
457 registration of a fair number of domain names, which might now be prohibitive under
458 the AGP Limits Policy.
459
460

461

462 5.2.3 Recommendations

463

464 It is unclear to what extent front-running happens, and the RAPWG does not recommend policy
465 development at this time. The RAPWG suggests that the Council monitor the issue and consider
466 next steps if conditions warrant.

467

468

469 5.3 Gripe Sites; Deceptive, and/or Offensive Domain Names

470

471 **5.3.1 Issue / Definition**

472 The issue is whether the registration these kinds of domain names are simply a form of
473 cybersquatting or whether the registration of such domain names should be addressed as a
474 separate form of registration abuse, and whether a consistent policy framework addressing this
475 category can or should be applied across all ICANN-accredited registries and registrars.

- 476 • Gripe/Complaint Sites a.k.a. “Sucks Sites”: Web sites that complain about a company’s
477 or entity’s products or services and uses a company’s trademark in the domain name
478 (e.g. companysucks.com).
- 479 • Pornographic/Offensive Sites: Web sites that contain adult or pornographic content and
480 uses a brand holder’s trademark in the domain name (e.g. brandporn.com).
- 481 • Offensive strings: Registration of stand-alone dirty words within a domain name (with or
482 without brand names).
- 483 • Registration of deceptive domain names: Registration of domain names that direct
484 unsuspecting consumers to obscenity or direct minors to harmful content—sometimes
485 referred to as a form of “mousetrapping.”

486
487 **5.3.2 Background**

488 The RAPWG discussed the issue of whether the registration of these types of domain names
489 should be addressed as a unique category of registration, with discussions that centered on
490 several different areas:

491

492 i. Gripe/Complaint Websites:

493 Several members pointed to the freedom of speech laws (not only in the U.S. but
494 internationally) that govern gripe and complaint sites using a company’s trademark in the
495 domain name, and indicated that registration of these names should not be considered as a
496 separate abuse category but rather should be considered as potential cases of cybersquatting, if
497 anything. Other members also discussed the intrinsic value of gripe and complaint Web sites to
498 companies and organizations that are seeking to understand the problems that customers may
499 have with respect to their products or services. The WG noted that aggrieved parties could turn

500 to the courts and the UDRP to remedy any claims they may have with respect to the use of
501 trademarks in a domain name. There was some discussion that decisions have not been
502 consistent with respect to gripe and complaint sites, although it is generally understood that
503 that truthful statements in gripe and complaint sites are protected free speech. Examples
504 include:

- 505 • http://decisions.courts.state.ny.us/fcas/fcas_docs/2005oct/30060065920045sciv.pdf. A
506 U.S. court ruled that a disgruntled customer of an insurance firm cannot be sued for
507 defamation over statements he made on his “gripe site” because those statements are
508 protected free speech.
- 509 • http://www.acluva.org/docket/pleadings/lamparello_opinion.pdf - A U.S. Appeals Court
510 found that a Web site using the domain name fallwell.com, set up to criticize evangelist
511 Jerry Falwell, did not violate trademark laws. There was no likelihood of confusion, ruled
512 the Court.
- 513 • <http://www.wipo.int/amc/en/domains/decisions/html/2007/d2007-0731.html> - A figure
514 behind controversial business schemes failed in his bid to gain control of the .COM
515 Internet address consisting of his name. A site that criticizes his activities was allowed to
516 keep the name.
- 517 • <http://www.wipo.int/amc/en/domains/decisions/html/2005/d2005-0168.html> - The
518 domain name AirFranceSucks.com was transferred to Air France. But the airline's victory
519 at arbitration was not without controversy: panelists disagreed about what the word
520 'sucks' really means to Internet users.
- 521 • <http://www.wipo.int/amc/en/domains/decisions/html/2009/d2009-1077.html>- The
522 Panel noted that that the domain name Radioshacksucks.com was not redirected to a
523 “gripe” Web site, but was pointing to a Web site with various pay-per-click links mainly
524 aimed at directing visitors to competing third party commercial Web sites. The Panel
525 found for the Complainant and transferred the name.
- 526 • At least one article has criticized some of the current UDRP decisions in this area. That
527 article can be found at: [http://domainnamewire.com/2009/12/04/freedom-of-speech-](http://domainnamewire.com/2009/12/04/freedom-of-speech-a-concept-not-limited-to-yankees/)
528 [a-concept-not-limited-to-yankees/](http://domainnamewire.com/2009/12/04/freedom-of-speech-a-concept-not-limited-to-yankees/)
529

530 ii. Pornographic Websites/Registration of Offensive Strings:

531 There appears to be some distinction however between complaint and gripe sites and the
532 registration of offensive strings, and whether these should be treated differently. The
533 registration of complaint site names (a.k.a. “sucks sites”) appears to have a direct impact on
534 organizations and companies, while the registration of offensive words have a more direct
535 impact on consumers. A domain name that contains a brand and an offensive word and also
536 points to a Web site that contains pornographic content can tarnish the reputation and the
537 image of a company’s brand. In addition to court action, the UDRP is a tool that companies and
538 organizations can turn to turn to remediate this problem because of the presence of the brand
539 name. A recent article in Computerworld magazine²¹ discusses the increase in cybersquatting
540 abuse in general. The article points to the example of the Web site FreeLegoPorn.com that
541 began publishing pornographic images created with Lego toys. The trademark owner Lego Juris
542 AS filed a UDRP complaint with the World Intellectual Property Organization’s (WIPO)
543 Arbitration and Mediation Center, which ultimately ruled in its favor.

544
545 However, a domain name that is registered for the sole purpose of misleading a consumer can
546 be extremely harmful. For example, the U.S. government enacted the Truth in Domain Names
547 Act (18 USC Sec. 2252B), which makes it a crime to knowingly register a domain name with the
548 intent to mislead a person into viewing obscene material. It also makes it a crime to register a
549 domain name with the intent to deceive a minor into viewing harmful material. These domain
550 names generally encompass typos (but not always) of recognizable names and trademarks as a
551 means of confusing people into visiting objectionable Web sites. Moreover, a number of ccTLDs
552 maintain policies governing the registration of objectionable words, with at least one ccTLD
553 registry (.US) apparently preventing the registration of the “seven dirty words” as per a
554 government policy. (The United States Federal Trade Commission also regulates the use of
555 these seven words on broadcast television and radio stations in the U.S.)

- 1/2/10 14:58
Deleted: (Domain-name wars-Rise of the Cybersquatters)

- 1/2/10 14:57
Deleted: c

- 1/2/10 14:58
Deleted: That article can be found at:
http://www.computerworld.com/s/article/print/9134605/Domain_name_wars_Rise_of_the_cybersquatters?taxonomyName=Networking+and+Internet&taxonomyId=16

²¹

http://www.computerworld.com/s/article/print/9134605/Domain_name_wars_Rise_of_the_cybersquatters?taxonomyName=Networking+and+Internet&taxonomyId=16

556

557 The RAPWG discussed some of the practical business challenges that could be presented for a
558 registry to adopt a policy that blacklists all names that also contain some form of prohibited
559 word. For example, the RAPWG noted the difficulty in (i) trying to monitor the use of expletives
560 in different languages, (ii) continuing to adapt to the evolution of obscenities in the vernacular
561 of a specific language, and (iii) addressing “gaming” of the system in this area.

562

563 RAPWG members also pointed out that ccTLDs and gTLDs are not in equivalent positions in
564 these matters. ccTLD operators are associated with certain countries, and are usually obligated
565 to adhere to their governments’ directives and laws, which reflect varying local standards of
566 decency. In contrast, gTLDs are by definition global, and it would be difficult to determine
567 baselines and balances for issues involving free speech and morals. Members commented that
568 ICANN is not in a good position to enforce morals in relation to domain names. The issue was
569 effectively settled in .COM/.NET/.ORG in 1999.

570

571 The RAPWG members generally agreed that gripe site and offensive domain names that use a
572 brand owner’s trademark are adequately addressed in the context of Cybersquatting for
573 purposes of establishing consistent registration abuse policies in this area.

574

575 **5.3.3 Recommendations**

576

577 Recommendation 1:

578

579 **View A:** The URDP should be revisited to determine what substantive policy changes, if any,
580 would be necessary to address any inconsistencies relating to decisions on “gripe” names and to
581 provide for fast track substantive and procedural mechanisms in the event of the registration of
582 deceptive domain names that mislead adults or children to objectionable sites.

583

584 **View B:** Make no recommendation. There should not be a [policy process](#) to examine the UDRP
585 for carve-outs or exceptions for “gripe” sites, or for fast track substantive and procedural

1/2/10 14:59

Deleted: PDP

586 mechanisms to address the registration of deceptive domain names that mislead adults or
587 children to objectionable sites. Gripe site and offensive domain names [that use trademarks](#) are
588 adequately addressed in the context of cybersquatting and the UDRP for purposes of
589 establishing consistent registration abuse policies in this area. Creating special procedures for
590 special classes of domains may present problems.

591
592 Recommendation 2:

593
594 [View A: Registries should consider developing internal best practice policies that would restrict](#)
595 [the registration of offensive strings in order to mitigate the potential harm to consumers and](#)
596 [children.](#)

597
598 [View B: ICANN is not a good forum to make recommendations regarding moral standards.](#)
599 ["Potential harm to consumers" is a vague standard. The recommendation is problematic for](#)
600 [global TLDs, and it was a matter closed in .COM/.NET/.ORG many years ago.](#)

601

602 **5.4 Fake Renewal Notices**

603

604 **5.4.1 Issue / Definition**

605 Fake renewal notices are misleading correspondence sent to registrants from an individual or
606 organization claiming to be or to represent the current registrar. These are sent for a variety of
607 deceptive purposes. The desired action as a result of the deceptive notification is:

- 608 ▪ Pay an unnecessary fee (fraud)
- 609 ▪ Get a registrant to switch registrars unnecessarily (“slamming”, or illegitimate market-
610 based switching)
- 611 ▪ Reveal credentials or provide authorization codes to facilitate theft of the domain

612

613 **5.4.2 Background**

614 What is the ICANN issue?

Marika Konings 2/2/10 10:49

Deleted: .

- 615 • Transfer issue (deceptive/fraudulent practices on the part of a registrar/reseller)
- 616 o Pretending to be current registrar
- 617 o Creating a fraudulent transfer event
- 618 • Domain hijacking issue (in the case of a non-registrar reseller)
- 619 • WHOIS abuse issue (obtaining contact information through questionable means or in
- 620 violation of RAA section 3.3.6.4)

621
622 What is ICANN's role?

- 623 • If the perpetrator is a registrar or reseller, ICANN policy applies through the RAA.
- 624 • If the perpetrator is not a registrar/reseller, ICANN's role is still applies, but it falls into
- 625 the realm of IRTP, hijacking or WHOIS abuse.

626
627 For a number of case studies, please see [document at:](#)
628 <http://forum.icann.org/lists/gnso-rap-dt/msg00446.html>

- 1/2/10 15:11
Deleted: [complete with link to wiki].

629
630 **5.4.3 Recommendations**

631
632 [Recommendation 1 : The RAPWG recommends the initiation of a Policy Development Process](#)
633 [by requesting an Issues Report to investigate fake renewal notices.](#)

634
635 [Recommendation 2: The RAPWG recommends that the GNSO refer this issue to ICANN's](#)
636 [Contractual Compliance department for possible enforcement action.](#)

637
638 **5.5 Name Spinning**

- 1/2/10 15:14
Deleted: <#>Refer to RAA working group (for additional enforcement tools) .

639
640 **5.5.1 Issue / Definition**

641 This is the practice of using automated tools used to create permutations of a given domain
642 name string. Registrars often use such tools to suggest alternate strings to potential registrants
643 when the string that the person queries they is not available for registration. .
644

645

646 5.5.2 Background

- 647 | ▪ The main concern is that such tools may produce results that may infringe upon
- 648 | trademarked strings.
- 649 | ▪ There was agreement in the RAPWG that name spinning is a tool that can be used by
- 650 | people for both legitimate and illegitimate purposes. As such, name-spinning is not in
- 651 | and of itself abusive.
- 652 | ▪ As discussed in some other areas, a determination of whether or not a particular use of
- 653 | such software is dependent on the user's intent.
- 654 | ▪ Until a domain name is actually registered, the trademark infringement (and therefore
- 655 | any registration abuse) is purely hypothetical, and therefore not a subject for policy-
- 656 | making.
- 657 | ▪ As discussed in some other areas, a determination of whether or not a particular use of
- 658 | such software is dependent on the user's intent.
- 659 | ▪ Domain name registrations that infringe on trademarks may be addressed via the UDRP.

- 1/2/10 15:20

Deleted: I

- 1/2/10 15:20

Deleted: that

660

661 5.5.3 Recommendations

662 None.

663

664 5.6 Pay-per-Click

665

666 5.6.1 Issue / Definition

667

668 Pay per click (PPC) is an Internet advertising model used on Web sites, in which the advertiser
669 pays the host only when their ad is clicked. The concern raised was use of a trademark in a
670 domain name to draw traffic to a site containing paid placement advertising.

671

672 **5.6.2 Background**

673 The RAPWG had consensus that pay-per-click advertising is not in and of itself a registration
674 abuse, and that bad-faith use of trademarks in domain names is a Cybersquatting issue that can
675 be addressed under the UDRP. The abuse of a PPC system for illicit gain is most appropriately
676 addressed by the operator of the PPC advertising network (e.g. Google AdSense).

677

678 **5.6.3 Recommendations**

679 None.

680

681 **5.7 Traffic Diversion**

682

683 **5.7.1 Issue / Definition**

684 Use of brand names in HTML visible text, hidden text, meta tags, or Web page title to
685 manipulate search engine rankings and divert traffic.

686

687 **5.7.2 Background**

688 The RAPWG had consensus that this is a pure Web site use issue with no inherent relation to a
689 domain name or registration process, and is therefore out of GNSO policy-making scope.

690

691 **5.7.3 Recommendations**

692 None.

693

694 **5.8 False Affiliation**

695

696 **5.8.1 Issue / Definition**

697 Web site that is falsely purporting to be an affiliate of a brand owner.

698

699 **5.8.2 Background**

700 The RAPWG had consensus that this is a pure Web site use issue with no inherent relation to a
701 domain name or registration process, and is therefore out of GNSO policy-making scope.

702

703 **5.8.3 Recommendations**

704 None.

705

706 **5.9 Domain Kiting / Tasting**

707

708 **5.9.1 Issue / Definition**

709 [Registrants may abuse the Add Grace Period through continual registration, deletion, and re-](#)
710 [registration of the same names in order to avoid paying the registration fees. This practice is](#)
711 [referred to as “domain kiting.” This term has been mistakenly used as being synonymous with](#)
712 [domain tasting, but it refers to multiple and often consecutive tasting of the same domain](#)
713 [name.](#)

714

715 **5.9.2 Background**

716

717 [Bob Parsons appears to have introduced the term “domain kiting” in a blog post in 2006. In the](#)
718 [post he chose to call the activity “kiting”, but his definition described what later came to be](#)
719 [termed “domain tasting” \(as The Public Interest Registry did in its letter to Steve Crocker on](#)
720 [March 26, 2006\). This confusion of terms carried forward for some time as can be seen in a](#)
721 [MessageLabs report published several months later.](#)

722

723 [Eventually, the current definition of domain kiting \(the serial re-registration of a domain to get a](#)
724 [domain for free\) solidified. Domain tasting is a different practice, in which a registrant measures](#)
725 [the monetization potential of a domain during the Add Grace Period, and deletes it in AGP if the](#)
726 [domain is not worth keeping.](#)

727

728 [ICANN staff looked into domain kiting \(while developing the 2007 Issue Report on domain](#)

729 [tasting\) and could not find anything except anecdotal evidence of the activity. A RAPWG](#)
730 [member performed an analysis of the .INFO registry in 2008 and again in December 2009, and](#)
731 [did not find any examples of kiting. \[1\] However domain kiting was a factor in a broader](#)
732 [complaint brought by Dell and Alienware against various registrars and individuals in 2007](#)
733 [\[here's the link -- http://www.domainnamenews.com/images/dell_doc1.pdf\]](#)

735 5.9.3 Recommendations

736
737 [The RAPWG does not recommend policy development at this time. The RAPWG suggests that](#)
738 [the Council monitor the issue \(in conjunction with ongoing reviews of domain-tasting\) and](#)
739 [consider next steps if conditions warrant.](#)

740

Marika Konings 2/2/10 10:49

Deleted: Registrants may abuse the Add Grace Period for continual registration, deletion, and re-registration of the same names in order to avoid paying the registration fees. This practice is sometimes referred to as "domain kiting." This term has been mistakenly used as being synonymous with *domain tasting*, but it refers to multiple and often consecutive tasting of the same domain name. ICANN staff has received anecdotal reports that this type of activity is occurring, but does not currently have data to demonstrate definitively that domain kiting occurs or to what extent. -

The anecdotal reports received by the ICANN staff would indicate that: -
<#>Very few registrants engage in kiting; -
<#>Those registrars who facilitate kiting are discovered and warned by the registry to cease the behaviour; -
<#>Kiting practices cannot enable a registrant to "keep" a single domain name. Any name is available to be taken in the drop pool by another registrant. The activity is only practicable if attempting to maintain a number of names – some would be lost at each drop. -

<#>Background -
Bob Parsons appears to have introduced the term "domain kiting" in a blog post in 2006. In the ... [1]

Marika Konings 2/2/10 10:49

Deleted: i

Marika Konings 2/2/10 10:49

Deleted: ssue R

Marika Konings 2/2/10 10:49

Deleted: r

Marika Konings 2/2/10 10:49

Deleted: eport on domain tasting) and could not find anything except anecdotal evidence of the activity. A RAPWG member performed an analysis of the .INFO registry in 2008 and again in December 2009, and did not find any examples of kiting.²² -

<#>Recommendations - ... [2]

Marika Konings 2/2/10 10:49

Deleted: <#>Refine the definitions of tasting and kiting based on the discussion and defined boundary conditions above. -
<#>Incorporate these definitions in any review or refinement of excess-delete policy and data collection or data reporting efforts. -
<#>Alert ICANN staff to the possibility of kiting ... [3]

Marika Konings 2/2/10 10:49

Deleted: It is unclear to what extent domain kiting happens, and the RAPWG does not recommend policy development at this time. The RAPWG suggests that the Council monitor the issue and consider next steps if conditions warrant. -

740 6. Malicious Use of Domain Names

741 The WG discussed how these problems relate to the scope of the Working Group’s activities as
742 well as GNSO policy-making. In general, the RAPWG found that malicious uses of domain names
743 have limited but notable intersections with registration issues.

744

745 The RAPWG acknowledges that e-crime is an important issue of the ICANN community. The
746 Internet community frequently voices concern to ICANN about malicious conduct and, in
747 particular, the extent to which criminals take advantage of domain registration and name
748 resolution services. Various parties—including companies, consumers, governments, and law
749 enforcement—are asking ICANN and its contracted parties to monitor malicious conduct and,
750 when appropriate, take reasonable steps to detect, block, and mitigate such conduct. The
751 question is what ICANN can reasonably do within its mission and policy-making boundaries.

752

753 6.1 Issue / Definition

754

755 The RAPWG was asked by the GNSO Council to examine issues surrounding illicit uses of domain
756 names, an outgrowth of learning done about that topic in the Fast-Flux Working Group (FFWG).
757 Specifically, the GNSO Council resolved:

- 758 • “The Registration Abuse Policy Working Group (RAPWG) should examine whether
759 existing policy may empower Registries and Registrars, including consideration for
760 adequate indemnification, to mitigate illicit uses of Fast Flux,” and
- 761 • “To encourage ongoing discussions within the community regarding the development of
762 best practices and / or Internet industry solutions to identify and mitigate the illicit uses
763 of Fast Flux.”²³

764

²³ <http://gnso.icann.org/meetings/minutes-03sep09.htm>

765 Malicious or illicit behavior may be mitigated by stopping the domain name from resolving. This
766 can be accomplished by the sponsoring registrar or registry by: applying an EPP Hold status; by
767 removing or changing the nameservers delegated to the domain; or by deleting the domain
768 name. Some malicious behaviors may be stopped by the hosting provider, and that may be the
769 most appropriate action depending upon the specific case. (For example, hosting providers can
770 take down individual phishing pages while the rest of the Web site continues to resolve.) But in
771 the ICANN context, stopping resolution of the domain is the relevant issue, since that is what
772 registrars and registries have the technical ability to make happen.

773

774 This issue is common to many types of abusive or malicious behavior – not only illicit fast-flux,
775 but also spamming, malware distribution, online child pornography, phishing, botnet command-
776 and-control, 419 scams, and others. Some specifics related to some common malicious abuses
777 are noted below.

778

779 The RAPWG also discussed how the basic accessibility of WHOIS, the accuracy of contact data,
780 and the use of proxy contact services are registration issues related to the malicious use of
781 domain names.

782

783 **6.2 Background**

784

785 ICANN possesses a limited technical coordination function for the DNS. The Internet is a huge
786 and sprawling environment that crosses international borders. It is decentralized by design, and
787 involves millions of parties all exercising ownership of or control over various assets and
788 infrastructure. These parties include network and telecom operators, ISPs, RIRs, registrants,
789 registrars, registry operators, corporations and organizations, governments, the root operators,
790 and more. The Internet and its users also depend upon hardware and software vendors, such as
791 the creators of operating systems and Web browsers. All of these parties are vulnerable to and
792 are often leveraged by criminals. As a result, no one party -- and no one type of entity -- has the
793 power to solve the problem of e-crime alone. Indeed, security experts agree that e-crime cannot

794 be solved – it can only be fought, and hopefully contained, just like offline crime. In the end, all
795 responsible parties have a role to play. Collaboration, data sharing, and education are effective
796 and important tools for dealing with Internet security problems.

797

798 Law enforcement becomes involved in only a tiny percentage of e-crime incidents, due to the
799 limited resources available, the large number of incidents, and the difficulties of investigating
800 and prosecuting across national borders and jurisdictions. Instead, the great bulk of abusive or
801 criminal behavior is dealt with via terms of service and contractual rights. The standard
802 mitigation model on the Internet is that malicious behavior is reported to the service provider(s)
803 who may have the right and ability to do something about it. Malicious domain name use is
804 reported to the relevant hosting provider and/or to the sponsoring registrar (and occasionally to
805 the registry operator). The registrar is the ICANN-related party with the direct relationship
806 with—and a direct contract with—the registrant. The registrar (and/or registry) may determine
807 if the use violates its legal terms of service, and decides whether or not to take any action.

808

809 Registrars always include language in their registrar-registrant contracts that allows the registrar
810 to suspend or cancel a domain name. The language and terms vary among registrars, and the
811 RAPWG examined this in its explorations of contract uniformity. Generally, registrars can act if
812 the registrant violates the registrar’s terms of service, or violates ICANN policy, or if illegal
813 activity is involved, or if payment fails. Some registrar-registrant agreements are broader and
814 allow the registrar to suspend a domain at any time for any reason, or for no reason. It appears
815 that registrars are empowered to mitigate abusive uses of domains if they so choose, and
816 indeed registrars use that freedom to suspend gTLD domains as a matter of daily business.

817

818 Some registrars may have terms that address specific domain name uses or abuses. For
819 example, the RAPWG saw how GoDaddy’s Universal Terms of Service contains a fairly unique
820 prohibition against use of domain names for “activities associated with the sale or distribution
821 of prescription medication without a valid prescription.”²⁴ Some RAPWG members commented

²⁴ <http://www.godaddy.com/gdshop/agreements.asp>

822 that such contractual variances are a way that registrars differentiate themselves in the market,
823 and they can help registrars adhere to the laws of the jurisdictions in which they are
824 incorporated or operate.

825

826 Some gTLD and ccTLD registry operators also have anti-abuse policies or provisions. Neustar's
827 .BIZ contract with ICANN require that "The registered domain name will be used primarily for
828 bona fide business or commercial purposes," and Neustar has relied on that requirement to
829 suspended domains being used for phishing and malware distribution. Anti-abuse policies have
830 also been instituted at the initiative of registry operators. For example, both The Public Interest
831 Registry (.ORG) and Afilias (.INFO) instituted policies under their existing rights in their ICANN-
832 registry and RRA contracts.^{25, 26} The resulting anti-abuse policies include lists of prohibited
833 abuses and reiterate the registry's right to suspend domain names. To create these anti-abuse
834 policies, the registry operators relied upon contract provisions that allow the registry operator
835 to "establish operational standards, policies, procedures, and practices for the Registry TLD", in
836 a non-arbitrary manner and applicable to all registrars, and consistent with ICANN's standards,
837 policies, procedures, and practices and the registry's Agreement with ICANN. Most ICANN-
838 registry contracts contain provisions such as the ones relied upon by the .INFO and .ORG
839 registries.

840

841 | So, it appears that all registrars and most, if not all registries are already empowered to develop
842 anti-abuse policies and mitigate malicious uses if they wish to do so. In addition, they may use
843 the Expedited Registry Security Request (ERSR, discussed below) to address threats to the DNS
844 or their TLDs.

845

²⁵ See: http://www.pir.org/index.php?db=content/Website&tbl=About_Us&id=14 and section 3.5.2 of the .ORG Registry-Registrar Agreement (RRA) at <http://www.icann.org/en/tlds/agreements/org/appendix-08-08dec06.htm>

²⁶ See http://www.info.info/info/abusive_use_policy and section 3.5.2 of the .INFO Registry-Registrar Agreement ("RRA") at <http://www.icann.org/en/tlds/agreements/info/appendix-08-08dec06.htm>

846 Some malicious uses of domain names involve legitimate domain name registrations that are
847 compromised or infected by criminals and then used to perpetrate crimes such as phishing and
848 malware. The RAPWG notes that any policy or recommendations must not adversely impact
849 innocent parties, including the registrant and the registrar.

850

851 RAPWG members also noted that malicious use of domain names varies significantly by TLD, and
852 some gTLDs have low-to-nonexistent problems. Many factors might explain this, including:
853 eligibility or locus requirements; general availability; price; the registrars the TLD is available
854 through and whether any of those registrars maintains less-than adequate [defences](#) or response
855 capabilities; and the general whims of e-criminals. This raises the question of whether “one-
856 size-fits-all” policies are relevant or needed. A WG member suggested that verification of users
857 might be a potential approach to consider suitable for policy development, while others felt that
858 required pre-screening of registrants raises many operational and economic issues.

859

860 It was pointed out that as a business practice, some registrars suspend or delete domain
861 registrations that have not been used for phishing, malware, etc. when they discover that the
862 registrant is using at least some of their domains for malicious purposes. In these cases, the
863 registrant has broken the terms of service agreement.

864

865 It was suggested that injecting uniform requirements can sometimes be counterproductive – it
866 can inject limitations into a situation where flexibility is often required, and might tie the hands
867 of registries and registrars by reducing or limiting their ability to effectively respond. It was
868 suggested that best practices or minimum standards could be explored. The importance of due
869 process was also noted.

870

871 **6.3 Intent, Risk, and Indemnification**

872

873 The decision to suspend a domain name is up to the discretion of the registrar or registry
874 operator, as per their terms of service. Suspending domain names involves risk. Registrars and
875 registry operators especially wish to avoid suspending the domain names of innocent parties (a

Marika Konings 2/2/10 11:32

Deleted: defenses

876 “false-positive”). A mistake can take an innocent registrant’s Web site and e-mail offline and
877 potentially cause significant economic damage and other problems for the registrant. In turn,
878 the registrar or registry operator may face legal action, and may further face customer service
879 and public relations problems.

880

881 The RAPWG’s members also discussed the issue of registration intent. It was agreed that
882 assessing what a domain name will be used for at the time of its registration requires
883 speculation about future intent, which can never be accurate 100% of the time. Some members
884 suggested that if one was able to determine at the time of registration that a domain name will
885 be used for an abusive activity, it might then be considered registration abuse. Some stated that
886 it is not possible to reliably determine at the time of registration whether a domain will be used
887 for phishing, spam or malware. Members provided examples of when it has been possible to
888 predict intent to a high degree of confidence, such as in certain cases of ongoing criminal
889 behavior. Such cases seem somewhat rare, the particulars can vary greatly between cases and
890 over time, and they usually involve small numbers of gTLD domains – perhaps dozen to
891 hundreds over time.²⁷ So for these reasons, even if such cases were determined to be
892 registration abuse, there were doubts that they would be good candidates for ICANN policy-
893 making.

894

895 Diligent registrars and registries have procedures for investigating abuse claims. These involve
896 performing diligence and documenting problems as a way to protect registrants and minimize
897 false-positives, to avoid risk, or to balance risk with the benefits of stopping malicious behavior.
898 Some registrars and registries may avoid risk by declining to suspend domains at all, or only in
899 the most pressing circumstances. Some may see domain name use as an issue they should not

²⁷ An example are the domains registered by the “Rock Phish” and “Avalanche” phishing operations. These gTLD and ccTLD domains were registered regularly, in batches, and contained characteristic string patterns. The case of Conficker was unusual in that it involved thousands of *unregistered* gTLD domain strings over time; see the commentary of Conficker and the Expedited Registry Security Request Process (ERSR) elsewhere in this paper.

900 make judgments about at all. As far as is known, there are no registrars or registry operators
901 that trust heuristics or abuse blacklists in order to automatically suspend abusive domain
902 names. Apparently all require the decisions to be made by an authorized person. Often this
903 function resides with an attorney, a compliance officer, or a specially trained analyst.

904

905 WHOIS data is an integral part of the investigation process used by registrars, registry operators,
906 law enforcement, and many other parties affected by malicious use of domains. The RAPWG
907 discussed how the basic accessibility of WHOIS, the accuracy of contact data, and the use of
908 proxy contact services are registration issues related to the malicious use of domain names.
909 Accessibility of WHOIS data is discussed elsewhere in this paper, and upcoming GNSO studies
910 will investigate how the contact accuracy and proxy issues are related to e-crime.

911

912 The Fast-Flux Working Group also discussed the issues of false-positives and intent. The FFWG
913 examined case studies that show that fast-flux detection systems create false-positives, and that
914 it is not always possible to determine the intent that some fast-flux domains are being used for.
915 There was discussion of how detection systems would need to yield an “acceptably low” level of
916 false-positives, but no agreement about what that level would be. Also, “In order to constrain
917 the working definition of fast flux to lie within the scope of ICANN to address, the FFWG also
918 tentatively agreed to limit the definition to the operation of the DNS and its registration system,
919 specifically excluding the question of what constitutes criminal intent.”²⁸

920

921 Along with the provisions that allow them to suspend domains names, registrar and registry
922 contracts include indemnification language. Current ICANN-registry and registry-registrar
923 contracts—and virtually all registrar-registrant agreements—obligate registrants to abide by
924 ICANN, registry, and registrar policies, and require registrants to indemnify and hold harmless

²⁸ “Final Report of the GNSO Fast Flux Hosting Working Group”, page 26:

<http://gns0.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf>

925 registrars and registries for enforcing those policies.²⁹ This language is designed to protect the
926 registrar or registry from claims and damages brought by the registrant.

927

928 An issue raised in the RAPWG is that indemnification language may not always an effective or
929 practical protection. Despite indemnification language, gTLD registries and registrars have been
930 sued by registrants for enforcing their terms of service.³⁰, ³¹, ³² Such legal proceedings can have

²⁹ For example, the .COM Registry-Registrar contract that is part of VeriSign's contract with ICANN says:
"2.14. Indemnification Required of Registered Name Holders. In its registration agreement with each
Registered Name Holder, Registrar shall require each Registered Name holder to indemnify, defend and
hold harmless VNDS, and its directors, officers, employees, agents, and affiliates from and against any and
all claims, damages, liabilities, costs and expenses, including reasonable legal fees and expenses arising
out of or relating to the Registered Name holder's domain name registration."

<http://www.icann.org/en/tlds/agreements/verisign/appendix-08-01oct08.pdf>

³⁰ In *Davies v. Afilias Ltd.*, 293 F.Supp.2d 1265 (M.D. Fla. 2003), a registry operator was sued in a U.S.
district court for locking Sunrise domains that the registrant did not have a right to possess, even though
the registrant was bound to relevant terms and conditions and had indemnified the registry operator. In
the course of the action, it was claimed that defendant Afilias incurred approximately US\$100,000 in
damages as a result of responding to the action. The court found that: "Plaintiff did not follow these rules,
but rather subverted the process by attempting to register domain names for his own use before the
names were offered on any basis to the general public, Defendant's 'interference' by locking the domain
names was, as a matter of law, justified....summary judgment in Defendant's favor is appropriate."

http://scholar.google.com/scholar_case?case=10308248522650356354&q=%222293+F.+Supp.+2d+1265%22&hl=en&as_sdt=2002

³¹ See *Stephen Weingrad and Weingrad & Weingrad, P.C. vs. Telepathy, Inc., Network Solutions, Inc., and Namebay S.A.M.* (05 Civ. 2024 (MBM), United States District Court for the Southern District of New York; 2005 U.S. Dist. LEXIS 26952). In this case, a registrar was sued after performing standard renewal and redistribution operations. Registrar Network Solutions notified registrant Weingrad of the upcoming expiration of his domain name. Weingrad failed to renew and the domain expired. When offered, Weingrad then declined to pay Network Solutions a standard redemption fee to redeem the name. The domain eventually became available, and was registered by another registrar. Weingrad then sued Network Solutions. The case was dismissed, and the court noted that Weingrad was bound by the

931 significant costs in money and resources, even though the registry or registrar was within its
932 legal rights and may have thought that it had exercised good faith. And as referenced above,
933 registrars have suspended domain names within their rights and then encountered customer
934 and public relations problems, which have costs of their own. Indemnification language in
935 ICANN contracts may fall short of being a true legal “safe harbor,” which reduces or eliminates a
936 party's liability under the law.

937

938 The domain-takedown and indemnification issue may come down to this: If a registrar or
939 registry chooses to suspend a domain for malicious use, it is deciding to assume the risk and
940 bear responsibility for possible consequences. But ICANN apparently does not have the power
941 to require registries or registrars to suspend domain names for use issues, and if it did, then
942 provisions to fully protect the contracted party from exposure to harm incurred by
943 implementing ICANN-required mitigation procedures must be considered.

944

945 **6.4 The Expedited Registry Security Request (ERSR)**

946

947 The RAPWG discussed the new ERSR, which offers a flexible, contract-related response
948 mechanism for registries to respond to significant malicious threats to the DNS itself or a TLD's
949 operations.

Registration Agreement between him and Network Solutions. Network Solutions believed that it had acted within its Registration Agreement, and within ICANN policies. However, Network Solutions incurred over US\$80,000 in legal fees defending itself.

³² There are many examples of how registrars have encountered difficulties after suspending domain names as per legal requirements and/or the registrar's terms of service. A few include:

- http://www.nytimes.com/2008/03/04/us/04bar.html?_r=3&scp=1&sq=liptak&st=nyt&oref=slogin&oref=slogin
- http://en.wikipedia.org/wiki/Network_Solutions#Fitna_controversy
- http://en.wikipedia.org/wiki/Godaddy#Suspension_of_Seclists.org
http://en.wikipedia.org/wiki/Godaddy#Deletion_of_FamilyAlbum.com

950

951 The Expedited Registry Security Request (ERSR)³³ was developed to "provide a process for gTLD
952 registries who inform ICANN of a present or imminent security incident (hereinafter referred to
953 as "Incident") to their TLD and/or the DNS to request a contractual waiver for actions it might
954 take or has taken to mitigate or eliminate an Incident. A contractual waiver is an exemption
955 from compliance with a specific provision of the Registry Agreement for the time period
956 necessary to respond to the Incident. The ERSR has been designed to allow operational security
957 to be maintained around an Incident while keeping relevant parties (e.g., ICANN, other affected
958 providers, etc.) informed as appropriate."

959

960 The ERSR was a result of learning from the Conficker problem, and was published for public
961 comment in September 2009. The ERSR was included in the Draft Applicant Guidebook, draft 3
962 (DAG3) so as to be made available in new TLDs that may be introduced in the future.

963

964 The ERSR framework allows flexibility, which will be necessary for responding to the unknown
965 and possibly novel threats to the DNS or TLDs that may arise in the future. It also allows
966 registries to propose operational solutions that may be suited to the situation at hand, and to
967 the registry's technical and operational capabilities. For example, in the case of another
968 Conficker, registries could be allowed to perform relevant domain name blocking and/or
969 registration themselves, or could accommodate arrangements in which a trusted party would
970 register relevant domain names and would receive fee relief from ICANN and the registry. The
971 ERSR also provides for expedited action, and process that involves legal and security experts at
972 ICANN and the registry or registries involved.

973

974 **6.5 Other Notes**

975

³³ <http://www.icann.org/en/registries/ersr/>

976 Registrars are often viewed by the public as the key to successfully resolving malicious conduct
977 because the registrars directly interact with those registrants who misuse domain names, and
978 because registrars have freedom to set their terms of service.

- 979 • It has been observed that registrars' responses and defensive mechanisms vary widely
980 in effectiveness and timeliness, and that some registrars are much less inclined to
981 address e-crime than others.
- 982 • Registrars are the parties that generally possess the most information that can be used
983 to assess the trustworthiness of a registration and a registrant and can link it to
984 malicious behavior. These include credit-card data (criminals often use stolen
985 credentials; see below), the true registrant's identity (when protected by a proxy
986 contact or privacy service), the IP of the registrant, and what domains that registrant
987 has registered in other TLDs.
- 988 • RAPWG members observed that malicious use of domain names varies significantly by
989 sponsoring registrar.³⁴
- 990 • Members also discussed apparent recurrent abuse by resellers, which goes back to how
991 registrars deal with their various agents, how those agents are bound to ICANN policies,
992 and how registrars are held accountable for the actions of their resellers.

993

994 Some members of the Internet security community are convinced that a small number of
995 domain name registrars knowingly tolerate malicious abuse, or are actively involved in it. Such
996 cases need the attention of ICANN and its compliance department. A key question is what tools
997 are needed and are appropriate to deal with this worst-case behavior.

998

999 Given the above, the logical question is whether there are any registration-related policies that
1000 can be used to positively affect such problems.

1001

1002 **6.6 Examples of Malicious Uses**

1003

³⁴ For example, see <http://rss.uribl.com/nic/>

1004 **Phishing**

1005

1006 Phishing is a Web site fraudulently presenting itself as a trusted brand in order to deceive
1007 Internet users into divulging sensitive information (e.g. online banking credentials, email
1008 passwords). The goal of phishing is usually the theft of funds or other valuable assets. The great
1009 majority of domains used for phishing are compromised or hacked by phishers, and the
1010 registrants are not responsible for the phishing. Such cases are not registered for bad purposes
1011 and therefore present cases where there is no inherent registration issue, and where mitigation
1012 must be handled carefully.

1013

1014 RAPWG members Rod Rasmussen and Greg Aaron publish semi-annual Global Phishing Surveys
1015 via the Anti-Phishing Working Group.³⁵ Findings from these reports include these relevant to
1016 registration and use issues:

- 1017 • About 81% of domains used for phishing are compromised or hacked by phishers, and
1018 the registrants are not responsible for the phishing. These domains should therefore not
1019 be suspended, and mitigation must usually be performed by the hosting provider.
1020 “Malicious” domain registrations totalled about 5,591 domain names in all gTLDs and
1021 ccTLDs worldwide in the first six months of 2009. This was about 18.5% of the domain
1022 names involved in phishing.
- 1023 • Only about 3.5% of all domain names that were used for phishing contain a brand name
1024 or variation thereof, designed to fool visitors. Placing brand names or variations thereof
1025 in the domain name itself is not a favored tactic of phishers, since brand owners are
1026 proactively scanning Internet zone files for such names. Instead, phishers usually place
1027 brand names in subdirectories or on subdomains in an attempt to fool Internet users.

³⁵ The last three reports were: First Half 2009:

http://www.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2009.pdf, Second Half 2008:

http://www.apwg.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf, First Half 2008:

http://www.apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf

1028 Most maliciously registered domains were random strings, such as “hodfw42hj.com.es”,
1029 which offered nothing to confuse a potential victim.

- 1030 • Phishers are increasingly using subdomain services to host and manage their phishing
1031 sites. These services are below the level provided by registries and registrars, and use of
1032 subdomains is not subject to policies maintained by ICANN. Phishers use such services
1033 almost as often as they register domain names. Such attacks even account for the
1034 majority of phishing attacks in certain large TLDs. This trend shows phishers migrating to
1035 services that cannot be taken down by registrars or registry operators.
- 1036 • Phishing (and phishing using maliciously registered domains) varies greatly by TLD.
1037 Many factors may explain this, including general availability or nature of the TLD, price,
1038 the registrars the TLD is available through, and locus or eligibility requirements.

1039
1040 The RAPWG had consensus that phishing is generally a domain name use issue. Those cases that
1041 involve misleading use of brand names in the domain string may be treated as cases of
1042 cybersquatting.

1043

1044 **Spam**

1045 Spam is generally defined as bulk unsolicited e-mail. Spam may be sent from domains, and spam
1046 is used to advertise Web sites.

1047

1048 Statistics published by various service providers show that spam levels vary significantly by TLD
1049 and by registrar.³⁶

1050

1051 The RAPWG had consensus that spam is generally a domain name use issue. Those cases that
1052 involve misleading use of brand names in the domain string may be treated as cases of
1053 cybersquatting.

1054

³⁶ For example: <http://rss.uribl.com/tlds/> and <http://rss.uribl.com/nic/>

1055 **Malware / Botnet Command-and-Control**

1056

1057 Malware authors sometimes use domain names as a way to control and update botnets.

1058 Botnets are composed of thousands to millions of infected computers under the common

1059 control of a criminal. Botnets can be used to perpetrate many kinds of malicious activity,

1060 including distributed denial-of-service attacks (DDoS), spam, and fast-flux hosting of phishing

1061 sites.

1062

1063 Relevant malware (including that associated with Srizbi, Torpig, and Conficker) on these infected

1064 machines attempts to contact domains included on some sort of pre-determined list or

1065 generated via an algorithm. If the botnet's master has deposited instructions at one of these

1066 valid domains, the botnet nodes will download those instructions and carry out the specified

1067 malicious activity, or update themselves with improved code.

1068

1069 It is notable that especially in the case of Conficker, these lists were not domain names that had

1070 been created – the great majority of the domains strings had not yet been created as domain

1071 names. They were essentially domains that might be registered at some point in the future by

1072 the criminal in question. Further, some of the valid domains may already be registered to

1073 innocent parties by coincidence.

1074

1075 If the relevant domain name list or domain-generation algorithm is known, white-hat parties

1076 (such as security researchers, registries, and registrars) can register and/or monitor the relevant

1077 domains. In the case of Conficker, white-hat parties registered the domain names that could

1078 have been used for command-and-control, successfully disrupted the botnet, and prevented

1079 much of it from being updated or controlled. These parties also sinkholed traffic to those

1080 domains (directed traffic to nameservers the researchers controlled). This allowed them to

1081 identify the IPs of infected computers, thus estimating the size of the botnet and enabling

1082 mitigation and cleanup efforts.

1083

1084 There are several ways in which malware authors and botnet "herders" utilize domain names
1085 they control or plan to control at some point in conjunction with their schemes. The most
1086 common and well understood is using websites under domains they control to distribute new
1087 malware infections to victims. This is often done via social engineering, where the malware is
1088 disguised as something else. More and more, we are seeing so-called "drive-by" infections,
1089 where a malware author simply gets a victim to visit their site via a browser that is not fully
1090 patched or is vulnerable due to a "zero-day exploit". Malware authors are also using domain
1091 names to facilitate communication with infected machines and/or to actually control large
1092 botnets. Many different malware families use pre-defined "rendezvous" domain names that are
1093 hard coded into an initial downloaded piece of malware. These rendezvous domains will provide
1094 further instructions using some sort of communications method, that is often, but not
1095 necessarily web-based, to relay further instructions or to provide more malware to download to
1096 the infected machine. Typically, the malware author will need to register such domains prior to
1097 deployment of their code in the wild. Other, more sophisticated malware programs (e.g.
1098 Conficker, Srizbi, Torpig), use a pre-defined algorithm to get updates from domains based on the
1099 current time and perhaps other conditions. This allows malware authors to pick and choose
1100 when and what domains to register in order to provide more instructions or control their
1101 botnets.

- 1102 • Descriptions of Conficker can be found at the Conficker Working Group
1103 (<http://www.confickerworkinggroup.org>) and on Wikipedia:
1104 <http://en.wikipedia.org/wiki/Conficker>
- 1105 • Srizbi info is also at Wikipedia: http://en.wikipedia.org/wiki/Srizbi_botnet plus a write-
1106 up on the domain calculator it uses at ThreatExpert.com:
1107 <http://blog.threatexpert.com/2008/11/srizbis-domain-calculator.html>.
- 1108 • A relevant research paper is: "Your Botnet is My Botnet: Analysis of a Botnet Takeover"
1109 by researchers at the University of California, Santa Barbara:
1110 <http://www.cs.ucsb.edu/%7Eseclab/projects/torpig/torpig.pdf>.
1111 Section 3 of this paper contains a very useful description of how the Torpig bot is
1112 controlled via domain names. The Conficker botnet uses a similar means. As the Santa
1113 Barbara authors note, "The use of domain flux in botnets has important consequences

1114 in the arms race between botmasters and defenders. From the attacker's point of view,
1115 domain flux is yet another technique to potentially improve the resilience of the botnet
1116 against take-down attempts. More precisely, in the event that the current rendezvous
1117 point is taken down, the botmasters simply have to register the next domain in the
1118 domain list to regain control of their botnet. On the contrary, to the defender's
1119 advantage, domain flux opens up the possibility of sinkholing (or "hijacking") a botnet
1120 [such as Torpig](#)." The Conficker bot is protected by sophisticated encryption, and its
1121 nodes will only download instructions from a domain that provides an authenticated
1122 response.

1123

1124 Newer variants of Conficker generate 50,000 potentially viable domains per day, spread across
1125 more than 100 TLDs. Registering all the domains generated by Conficker at market prices would
1126 therefore carry an enormous cost. (The Santa Barbara team estimated the cost at between
1127 \$91.3 million and \$182.5 million per year.)

1128

1129 Some registries blocked the viable Conficker domains. Those registries refused all attempts to
1130 create the relevant domains, thereby keeping them out of the hands of all parties for a certain
1131 period of time. Some registry operators were able to accomplish blocking, while others were not
1132 able to do so due to technical or policy reasons.

1133

1134 It is generally agreed by the members of the Conficker Working Group³⁷ that:

- 1135 1) Fighting Conficker by acquiring and/or blocking domains was a success in many ways and
1136 was worth attempting. The effort prevented many nodes from being updated or controlled,
1137 and many nodes were identified and removed from the botnet.
- 1138 2) The counter-measure of acquiring and/or blocking domains is probably not scalable in the
1139 long term. It is expected that criminals may expand the numbers of domains their malware
1140 algorithms use. The blocking efforts also depend upon the flawless and continued
1141 participation of all relevant TLD registry operators.

³⁷ <http://www.confickerworkinggroup.org>

1142 **6.7 Use of Stolen Credentials**

1143

1144 **6.7.1 Issue / Definition**

1145 Criminals often use stolen credentials—such as stolen credit card numbers—to register domain
1146 names for malicious purposes. Is this a registration issue, and what if any solutions can be
1147 pursued through ICANN?

1148

1149 **6.7.2 Background**

1150

1151 For the purposes of examining registration abuse and the “use of stolen credentials”, there are
1152 three usages that seem to apply:

- 1153 1. “Identity credentials” – Credentials that establish identity (e.g. personal identification cards,
1154 stored personal information)
- 1155 2. “Access credentials” – Credentials that control access to computer systems (e.g. username
1156 and password, digital certificates)
- 1157 3. “Financial credentials” – Credentials that provide access to financial accounts (e.g. credit
1158 and debit cards).

1159 Some blending of usages would apply in some cases as well. For example, the use of a stolen e-
1160 mail account to establish identity or the authority to modify access to financial credentials
1161 crosses multiple definitions.

1162

1163 Given the disparate nature of the uses and protections against abuse the types of credentials
1164 identified each have, it would seem prudent to examine them individually. Some commonalities
1165 may present themselves to allow for unified approaches.

1166

1167 *Identity Credentials*

1168 In general, stolen identity credentials allow a miscreant to assume or impinge the identity of
1169 another in order to perpetuate one of their own schemes. This can manifest itself in the use of
1170 purloined personal information to make a domain registration appear to be legitimate (e.g. false

1171 WHOIS) or in allowing a perpetrator to assume control over access or financial credentials. The
1172 latter case can be explored in-depth in examining those other two credential types, but the
1173 former case is worth considering further.

1174

- 1175 1. Fraudsters use misappropriated identities of the actual individuals or institutions targeted
1176 by a particular scheme in conjunction with a domain registration. The fraudster wishes to
1177 make the domain name appear to be associated with the actual victim in order to make
1178 their scheme more viable to other victims, and/or their application for the domain
1179 legitimate.
- 1180 2. Miscreants use identities of random, but real individuals/organizations in conjunction with a
1181 domain registration, unrelated to the actual fraud scheme. Use of real data may allow the
1182 miscreant to fool anti-fraud measures put in-place by the registrar. Victims of the actual
1183 scheme may be put at ease by the appearance of “real” verifiable domain ownership
1184 information in WHOIS, or they may make complaints against innocent parties. The stolen
1185 identity data may well cause delays in authorities investigating the scheme, as innocent
1186 parties are scrutinized. The person who is “spoofed” in this instance may be the registrant
1187 for other domains, which may also allow the registration to get past anti-fraud measures,
1188 especially if the registrar being used is the same.
- 1189 3. The miscreant uses stolen identities in conjunction with stolen financial credentials to
1190 bolster their fraud efforts when registering a domain. Including the stolen access
1191 information in WHOIS and/or account information that matches stolen credit card data can
1192 help avoiding anti-fraud systems, as well as all the benefits mentioned above.

1193

1194 *Access Credentials*

1195 A miscreant can do quite a bit of damage with stolen access credentials. Outside of reselling
1196 those credentials, the real value of stolen access credentials lies in what is possible to do with
1197 the systems to which those credentials provide access. Two possible attacks seem to be
1198 meaningful within the confines of “domain registration abuse” examined here. First are direct

1199 attacks against registrar/reseller systems using stolen access credentials for that service.

1200 Second, a perpetrator could launch an indirect attack via access credentials to other accounts.

1201

1202 1. A miscreant with direct access to a domain management account can make new domain
1203 registrations using funds or “credits” that account may have with the reseller or registrar.

1204 Obviously domains can be taken over, deleted, or otherwise sabotaged from such a
1205 compromised account, but those scenarios are likely outside the scope of “registration
1206 abuses”. Further, a miscreant may be able to gain access to credit card information that is
1207 stored in such an account, or affect purchases with that card that directly benefit that
1208 criminal. Again, this is outside scope, as this is more of a theft problem than a domain
1209 registration issue, but it is likely a concern that could come up in discussions of this topic.

1210 2. If a fraudster has access to an account that is used to verify identity or confirm change
1211 requests, like an e-mail account, they can either attempt to gain access/control over a
1212 domain management account, or use a domain registration verification process to register
1213 domains using someone else’s account/identity. Some domain resellers may use legacy
1214 models based on the original e-mail based registration and modification system, which
1215 would allow for fraudulent domain registrations based on e-mail confirmations.

1216 3. If a criminal has access via stolen credentials (or simply hacking) into a computer/server that
1217 is part of some automated domain registration system, they can subvert that system. With
1218 such control, new domains can be registered using the victim’s automated access to
1219 registrar systems. Of course hijacking, sabotage, and other acts can be perpetuated as well,
1220 just as if the miscreant had access to an account with the registrar/reseller.

1221

1222 *Financial Credentials*

1223 Abuses perpetrated with stolen financial credentials are fairly straightforward. The criminal can
1224 utilize those credentials to fraudulently register domains and other related resources. This is
1225 quite common practice with criminals today, with most of the domains registered in this manner
1226 being used to perpetuate other crime, fraud, and abuse. Such credentials include credit cards,
1227 debit cards, on-line banking, alternate payment systems (e.g. PayPal), ACH systems, and other
1228 various means for affecting payments for domain name transactions.

1229

1230 An interesting aspect for domain name registration via stolen financial credentials versus other
1231 types of fraud done via stolen financial credentials is the need to establish domain ownership
1232 information (whois and/or account) and domain deployment characteristics (nameservers) at
1233 the time of registration. This allows for some unique techniques to expose fraudulent
1234 registrations via stolen financial credentials.

1235

1236 *Observed abuses*

1237 Use of stolen financial credentials would seem, at first glance, to be the primary abuse seen
1238 today. Thousands of domains are registered daily using such credentials to perpetuate all sorts
1239 of criminal and abusive schemes. However, there has been a shift of late in the way criminals
1240 are amassing infrastructure resources, with more emphasis being placed on obtaining access
1241 credentials to infrastructure elements. Some level of stolen identity credential abuse co-exists
1242 with these other abuses as well, so all three areas deem at least some consideration.

1243

1244 *Roles for policy and other industry-wide approaches*

1245 These three types of uses of stolen credentials present different opportunities for mitigation
1246 efforts, both at the individual registrar/reseller level and across the industry. Some registrars
1247 and resellers see fairly frequent abuse, especially of stolen financial credentials, while others do
1248 not. There are opportunities for dissemination of best practices, plus potential for “minimum
1249 standards” for dealing with various types of abuse in this arena. Further, given the unique
1250 nature of domain names requiring access to a shared data system (the zone files) with detailed
1251 ownership/contact data in order to function and be in compliance, there may be ways to share
1252 information about fraudulent activities occurring at some registrars/resellers to curb those
1253 abuses across the industry. No formal system or policy for the latter currently exists.

1254

1255 Free-market forces have largely determined how different registrars and their resellers respond
1256 to these issues. There is a strong argument for allowing competition to dictate many of these
1257 responses, as there is continuous innovation in these areas, and many market participants

1258 compete on these features. And there is a strong argument that is an apparent free-market
1259 failure, in which registrars/resellers who appear to be fairly weak in practices to prevent such
1260 fraudulent registrations are generally not being penalized. The large numbers of fraudulent
1261 domains obtained through the methods discussed previously with infrequent sanctions
1262 evidences this. So the question becomes one of balance, as is often the case in such industry
1263 issues.

1264

1265 Complicating these issues are the large number of business models currently employed by
1266 domain registration companies. "Retail" registrars who sell direct to individuals and businesses
1267 will most often process transactions with credit cards or alternate payment services. There are
1268 many other models, including large "corporate" registrars that establish credit accounts, multi-
1269 level resellers, internal operations that register names on their own accounts, and more. This
1270 makes it more difficult to find solutions that effectively cover all vendors well. Perhaps
1271 concentrating on the areas that appear to have the highest incident of abuses would be
1272 prudent.

1273

1274 6.7.3 Recommendations Regarding Malicious Use of Domain Names

1275

1276 The RAPWG recommends the creation of non-binding best practices to help registrars and
1277 registries address the illicit use of domain names. This effort should be supported by ICANN
1278 resources, and should be created via a community process such as a working or advisory group
1279 while also taking the need for security and trust into consideration. The effort should consider
1280 (but not be limited to) these subjects:

- 1281 ○ Practices for identifying stolen credentials
- 1282 ○ Practices for identifying and investigating common forms of malicious use (such
1283 as malware and phishing)
- 1284 ○ Creating anti-abuse terms of service for inclusion in Registrar-Registrant
1285 agreements, and for use by TLD operators.
- 1286 ○ Identifying compromised/hacked domains versus domain registered by abusers

- 1/2/10 15:30
Deleted:

- 1/2/10 15:31
Deleted: e

- 1/2/10 15:31
Deleted: s

1287
1288
1289
1290
1291
1292
1293
1294
1295
1296

- Practices for suspending domain names
- [Account access security management](#)
- Security resources of use or interest to registrars and registries
- [Survey registrars and registries to determine practices being used, and their adoption rates.](#)

- 1/2/10 15:34
Deleted: s

- 1/2/10 15:35
Deleted: Addressing use of Stolen Access Credentials

- 1/2/10 15:36

Deleted: Whois

1296 7. WHOIS Access

1297

1298 7.1 Issue / Definition

1299

1300 The RAPWG found that the basic accessibility of WHOIS has an inherent relationship to domain
1301 registration process abuses, and is a key issue related to the malicious use of domain names. It
1302 appears that WHOIS data is not always accessible on a guaranteed or enforceable basis, is not
1303 always provided by registrars in a reliable, consistent, or predictable fashion, and that users
1304 sometimes receive different WHOIS results depending on where or how they perform the
1305 lookup. These issues interfere with registration processes, registrant decision-making, and with
1306 the ability of parties across the Internet to solve a variety of problems.

1307

1308 WHOIS is an area within GNSO policy-making scope and has had a long history of discussion.

1309 Below, the RAPWG comments on the basic availability of and access to WHOIS data, and not the
1310 accuracy of contact data or the use of proxy contact services. To avoid duplication of effort and
1311 charter scope problems, the RAPWG decided to identify when WHOIS is seen to be a
1312 contributing factor in other problems, and not to discuss WHOIS issues for which the GNSO has
1313 already commissioned studies. (Those are: WHOIS contact data accuracy, the use of proxy
1314 contact and privacy services, implications of non-ASCII registration data in WHOIS records, and
1315 technical requirements for the WHOIS service itself – including potential replacements. For
1316 background, please see: <http://gns0.icann.org/issues/whois/>)

1317

1318 WHOIS data availability problems have been discussed in other GNSO working groups, for
1319 example:

- 1320 • The Post-Expiration Domain Name Recovery Working Group (PEDNR-WG) discussed how
1321 access to WHOIS data is essential for parties to determine if contact data has been
1322 updated upon the expiration of a domain name, and to check domain name expiration

1323 dates. A majority of the registrars polled may make substantial updates to WHOIS data
1324 upon expiration.³⁸

1325 • The Inter-Registrar Transfer Policy Part A PDP Working Group (IRTP-WG)³⁹ noted in its
1326 final report that gaining registrars sometimes have difficulty accessing WHOIS data, and
1327 therefore Administrative Contact e-mail addresses.

1328 • The Fast-Flux PDP Working Group (FFWG) discussed how responders must access
1329 WHOIS data when mitigating illicit uses of domain names.

1330

1331 Published WHOIS data for domain names involved in malicious conduct is an irreplaceable part
1332 of the investigation and mitigation processes used by registrars, registry operators, registrants,
1333 security companies, brand owners, victims, and law enforcement.

1334 • The national law enforcement agencies of the United States, the United Kingdom,
1335 Australia, Canada, and New Zealand have recommended that “ICANN should require
1336 Registrars to have a Service Level Agreement for their Port 43 servers.” These
1337 authorities consider that this is required in order “to aid the prevention and disruption
1338 of efforts to exploit domain registration procedures by criminal groups for criminal
1339 purposes.”⁴⁰

³⁸ “Draft Initial Report on the Post-Expiration Domain Name Recovery Policy Development Process”:

https://st.icann.org/data/workspaces/post-expiration-dn-recovery-wg/attachments/post_expiration_domain_name_recovery_wg:20100112125658-0-27743/original/Draft%20Initial%20Report%20-%20PEDNR%20PDP%20-%2012%20January%202010.doc

³⁹ “Draft Final Report on the Inter-Registrar Transfers Policy - Part A Policy Development Process”:

https://st.icann.org/data/workspaces/irtp_jun08_pdp-wg/attachments/irtp_part_a_pdp_wg_pdp_jun08:20090318145458-1-14319/original/Draft%20Final%20Report%20-%20IRTP%20Part%20A%20-%2018%20March%202009.doc%20%5BCompatibility%20Mode%5D.pdf

⁴⁰ “Law Enforcement Recommended RAA Amendments and ICANN Due Diligence”, November 2009,

[https://st.icann.org/raa-related/index.cgi/LawEnforcementRAArecommendations%20\(2\).doc?action=attachments_download;page_name=05_january_2010;id=20091118185109-0-21002](https://st.icann.org/raa-related/index.cgi/LawEnforcementRAArecommendations%20(2).doc?action=attachments_download;page_name=05_january_2010;id=20091118185109-0-21002)

1340 • The Anti-Phishing Working Group’s DNS Policy Committee has stated that published
1341 WHOIS is “an invaluable resource, in fact, without which most of the cited cases would
1342 not have been successful. For cases in which legitimate machines or services have been
1343 hacked or defrauded, published domain name WHOIS information is an important tool
1344 used to quickly locate and communicate with site owners and service providers. For
1345 cases where domain names are fraudulently registered, the published domain name
1346 WHOIS information can often be tied to other bogus registrations or proven false to
1347 allow for quick shutdown.”⁴¹

1348

1349 **7.2 Background**

1350

1351 ICANN’s current registry contracts require registry operators to adhere to port 43 WHOIS Service
1352 Level Agreements (SLAs). These SLAs require that port 43 WHOIS service be highly accessible
1353 and fast. For example, the .ORG contract requires that WHOIS service be functional at least
1354 99.31% of the time per month (with exceptions for scheduled maintenance), and that responses
1355 be provided in less than 800 milliseconds. Failure of registries to meet these SLAs have been
1356 very rare according to monthly registry reports.⁴²

1357

1358 The majority of gTLD registries are “thick” registries, in which all authoritative WHOIS data—
1359 including contact data—is maintained at the registry. The .COM and .NET registries are “thin,”
1360 and contact data is located only at each domain name’s sponsoring registrar. Registrars are
1361 therefore responsible for providing WHOIS service for .COM/.NET names so that contact data
1362 may be retrieved. The .COM/.NET registry contains approximately 85% of the gTLD domains in
1363 existence,⁴³ so registrar WHOIS accessibility is very important. When displaying WHOIS data for

⁴¹ “Issues in Using DNS Whois Data for Phishing Site Take Down,”

http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf

⁴² <http://www.icann.org/en/tlds/monthly-reports/>

⁴³ “VeriSign Domain Name Industry Brief,” September 2009, <http://www.verisign.com/domain-name-services/domain-information-center/domain-name-resources/domain-name-report-dec09.pdf>

1364 thick TLD domains names—especially on their Web sites—registrars often query the registry’s
1365 WHOIS, and display that output to users.

1366

1367 The Registrar Accreditation Agreements (RAAs)⁴⁴ require that registrars provide:

- 1368 • port 43 WHOIS access
- 1369 • a Web-based WHOIS
- 1370 • a listed set of information (WHOIS data fields), including:
 - 1371 ○ identity of the registrar
 - 1372 ○ domain name’s expiration date
 - 1373 ○ nameservers associated to the domain; and
 - 1374 ○ specified fields of data for the Registrant Contact, Administrative Contact, and
1375 Technical Contact.

1376

1377 There are no service levels (SLAs) in the Registrar Accreditation Agreements (RAAs). A registrar-
1378 provided WHOIS service is not required to be online for any particular amount of time, nor
1379 provided with any particular response speed.

1380

1381 Port 43 is designed for use with automated and machine queries. It can also be queried
1382 manually by users who know how to perform telnet sessions and the “whois” command in
1383 Linux/Unix/macosx shell. The percentage of Internet users who are technically fluent enough to
1384 perform these types of queries (or even know about port 43 at all) is small. Thus, it is required
1385 that registrars have a Web-based WHOIS query on their sites.

1386

1387 A sub-team of RAPWG members performed some basic research by querying the Web-based
1388 and port 43 servers of 50 registrars. This set included the top 20 registrars by gTLD market
1389 share, 15 randomly-chosen mid-sized registrars, and 15 randomly-chosen small registrars.
1390 When a registrar’s site was in a language other than English, the assistance of a native speaker

⁴⁴ <http://www.icann.org/en/registrars/agreements.html>

1391 was obtained. In addition to manual checks, automated queries of port 43 were performed to
1392 test availability over time.

1393

1394 The sub-team members found WHOIS accessibility situations with 19 of the 50 registrars
1395 sampled. Four registrars may have been in violation of their contractual WHOIS access
1396 requirements:

- 1397 • Two did not provide a functional Web-based WHOIS.
- 1398 • One registrar's WHOIS listed a sponsoring registrar different from that provided by the
1399 .COM/.NET registry WHOIS. The registrar's port 43 server provided an expiration date
1400 different from that listed in the registry. The registrar's Web WHOIS provided two
1401 different expiration dates for the same domain name.
- 1402 • One registrar did not identify the sponsoring registrar of its domains. The registrar does
1403 not operate its port 43 server on the domain indicated by the .COM/.NET registry
1404 WHOIS; the registrar's WHOIS service is evidently subcontracted to a second registrar on
1405 that registrar's domain; and the sponsoring registrar's Web WHOIS is provided on a
1406 third domain not branded as the sponsoring registrar.

1407

1408 In addition, one registrar provided facially invalid registrant contact data for its own .COM name
1409 -- including a registrant contact e-mail address on the domain "icann.org". This appears to be a
1410 violation of the RAA.

1411

1412 Fifteen other registrars presented these situations:

- 1413 • Three registrars had port 43 servers that did not return replies for a notable number of
1414 queries. One was offline/nonresponsive 21% of the time, one was
1415 offline/nonresponsive 20% of the time, and one was offline/nonresponsive 14% of the
1416 time. (Based on 100 queries per registrar, spread out over several weeks).
- 1417 • Ten provided different WHOIS data on their port 43 servers than they did via their Web
1418 WHOIS.
 - 1419 ○ Four provided only thin contact data via their Web WHOIS, while providing thick
1420 contact data only on port 43.

- 1/2/10 15:37
Deleted: Two

- 1/2/10 15:37
Deleted: (based

- 1421 ○ In two cases, registrars provided two different expiration dates for each domain
1422 name via the Web WHOISes. One of the two expiration dates did not match the
1423 expiration date provided by the .COM/.NET registry.
- 1424 ○ Two sometimes provided full contact data on their Port 43 servers, and
1425 sometimes provided just Registrant contact data (and no Admin or Tech contact
1426 data) on their port 43 servers. It is unknown if this was due to a rate-limiting
1427 activity.
- 1428 ○ One registrar did not provide registrant contact data via port 43, and did not
1429 provide Admin or Tech contact data via its Web WHOIS.
- 1430 ○ One registrar provided a required data field (Tech and Admin contact phone
1431 numbers) on port 43 but not via its Web WHOIS.
- 1432 • Four cut off telnet sessions to port 43 very quickly--effectively disallowing manual
1433 queries via that method.
- 1434

1435 These results indicate that:

- 1436 1. Some registrars appear to be in violation of their contractual WHOIS accessibility
1437 obligations;
- 1438 2. Users are occasionally unable to obtain contact data due to WHOIS availability
1439 problems.
- 1440 3. Registrars occasionally provide registration data that differs from that provided by the
1441 registry.
- 1442 4. Users are sometimes given different registration data depending on the method they
1443 use to access the sponsoring registrar's WHOIS.
- 1444 5. Users are sometimes given different registration data depending upon who they are;
1445 perhaps depending upon whether they are being rate-limited.
- 1446

1447 These issues were distributed across a notable number of registrars, with different sizes,
1448 business models, and locations around the world.

1449

1450 The reasons why registrars provide different data on port 43 versus their Web sites requires
1451 further investigation. Some might be attempts to prevent automated data mining by spammers,
1452 competitors, and other parties. The RAPWG notes that reasonable rate-limiting WHOIS can be a
1453 valid, prudent practice – for example it can prevent spammers from mining WHOIS
1454 information⁴⁵, and can prevent WHOIS servers from being overwhelmed by excessive queries.
1455 During Web-based WHOIS sampling, the RAPWG members observed that only some registrars
1456 employ CAPCHAs on their Web-based WHOIS services as a protection against automated
1457 queries.

1458
1459 In addition to the research conducted by working-group members, the RAPWG requested
1460 information from the ICANN Compliance Department about how it monitors registrar WHOIS
1461 access. The ICANN Compliance Department noted: "ICANN has developed a Whois server audit
1462 tool which monitors access to registrars' Whois servers over a Port 43 connection. The script
1463 developed for this task retrieves data for 4 registered domain names for each accredited
1464 registrar.... The purpose of the audit is to flag Whois servers that are down for an amount of
1465 time that is suspect and probably not just a manifestation of periodic server maintenance or
1466 scheduled update. ... What is the "reasonable amount of time" for a server to be down?
1467 Probably no more than an hour or so per day, although these are ICANN internal, 'soft metrics',
1468 not agreed-upon timeframes with registrars. The script records the results and flags registrars
1469 that prevent access to data on registered names. Transient network problems are less of a
1470 concern, so ICANN focuses on long-term behavior, i.e., registrars which ICANN is unable to
1471 communicate with for several days in a row.ICANN also reaches out to registrars that provide
1472 access to data on registered names but provide 'thin', not 'thick', Whois data. The former does
1473 not provide details on the registered name holder and additional contacts, which is required by
1474 the RAA."⁴⁶

1475

⁴⁵ See: "SAC 023: Is the WHOIS Service a Source for

Email Addresses for Spammers?": <http://www.icann.org/en/committees/security/sac023.pdf>

⁴⁶ <http://forum.icann.org/lists/gnso-rap-dt/msg00454.html>

1476 Over the last three years, ICANN’s Compliance Department has sent seven escalated compliance
1477 notices (e.g. notices of breach, termination, or RAA non-renewal) to seven registrars for failure
1478 to comply with WHOIS access requirements of the Registrar Accreditation Agreement:

- 1479 • One registrar did not have its contract renewed solely for failure to provide WHOIS
1480 access. (South America Domains dba NameFrog.com, which had less than 300 gTLD
1481 names under sponsorship at the time.)
- 1482 • The other six registrars were cited for both WHOIS access breaches AND at least one
1483 other contract violation, such as failure to pay ICANN fees, failure to escrow data,
1484 and/or failure to respond to WHOIS accuracy complaints.

1485
1486 ICANN’s Compliance Department is in contact with registrars to resolve issues before escalated
1487 compliance notices become necessary. The Compliance staff noted to the RAPWG that “some
1488 registrars block incoming WHOIS queries traffic by IP address, and Compliance works with the
1489 registrars to get them unblocked when there may be a misunderstanding.” and, “Aside from
1490 metrics on informal outreach to resolve blocked Whois servers and incomplete, or ‘thin’, Whois
1491 data with registrars, which have been more than two dozen in the past 6-8 months, Compliance
1492 could provide bi-weekly statistics to the WG from here on out on the number of registrars that
1493 showed a pattern of restricting access to their Whois server over a Port 43 connection. These
1494 statistics have not been published before.”

- 1/2/10 15:38

Deleted: becomes

Mike O’Connor 20/1/10 09:34

Comment: Unpaired quote.

1495
1496 So, it appears that some contractual violations are cured in an amicable manner, and that public
1497 breach letters have apparently been used as a tool of last resort. It is unknown how many
1498 WHOIS accessibility issues have been discovered but not resolved.

- 1/2/10 15:38

Deleted: a friendly

1499
1500 The last time that ICANN published WHOIS access compliance data was 2007. That year,
1501 ICANN’s Compliance Department examined every ICANN-Accredited Registrar’s Web site, and
1502 did not examine port 43 access.⁴⁷

1503

⁴⁷ <http://www.icann.org/en/compliance/reports/contractual-compliance-audit-report-18oct07.pdf>

1504 The Compliance Department numbers indicate that WHOIS access problems are found regularly.
1505 Above and beyond those, the RAPWG research indicates that a notable percentage of registrars
1506 might not make WHOIS data available in a reliable, consistent, or predictable fashion.

1507

1508 **7.3 Recommendations**

1509

1510 | Recommendation 1. The GNSO should determine what additional research and processes may
1511 be needed to ensure that WHOIS data is accessible in an appropriately reliable, enforceable, and
1512 consistent fashion.

- 1/2/10 15:38
Deleted:

1513 | The GNSO Council should consider how such might be related to other WHOIS efforts, such as
1514 the upcoming review of WHOIS policy and implementation required by ICANN's new Affirmation
1515 of Commitments. The Affirmation of Commitments says: "ICANN additionally commits to
1516 enforcing its existing policy relating to WHOIS, subject to applicable laws. Such existing policy
1517 requires that ICANN implement measures to maintain timely, unrestricted and public access to
1518 accurate and complete WHOIS information, including registrant, technical, billing, and
1519 administrative contact information. One year from the effective date of this document [30
1520 September 2009] and then no less frequently than every three years thereafter, ICANN will
1521 organize a review of WHOIS policy and its implementation to assess the extent to which WHOIS
1522 policy is effective and its implementation meets the legitimate needs of law enforcement and
1523 promotes consumer trust."⁴⁸

- 1/2/10 15:39
Deleted: -

1524

1525 | Recommendation 2. The GNSO should request that the ICANN Compliance Department publish
1526 more data about WHOIS accessibility, on at least an annual basis. This data should include a)
1527 the number of registrars that show a pattern of unreasonable restriction of access to their port
1528 43 WHOIS servers, and b) the results of an annual compliance audit of compliance with all
1529 contractual WHOIS access obligations.

- 1/2/10 15:40
Deleted: restricting

- 1/2/10 15:39
Deleted: Whois

⁴⁸ <http://www.icann.org/en/announcements/announcement-30sep09-en.htm>

1530

1531

1531 8. Uniformity of Contracts

1532

1533 8.1 Issue / Definition

1534 Three specific charter objectives of the RAPWG were to:

- 1535 • Understand if registration abuses are occurring that might be curtailed or better
- 1536 addressed if consistent registration abuse policies were established,
- 1537 • Determine if and how {registration} abuse is dealt with in those registries {and
- 1538 registrars} that do not have any specific {policies} in place, and
- 1539 • Identify how these registration abuse provisions are {...} implemented in practice or
- 1540 deemed effective in addressing registration abuse.

1541

1542 The RAPWG formed a sub-team to fully appreciate the current state environment of ICANN-
1543 related contracts and agreements, and then discussed the findings in the larger RAPWG.

1544

1545 8.2 Background

1546 The Sub-Team was tasked with the specific topic of contract uniformity relative to abuse as
1547 defined by the larger Working Group, and presented its research to the larger WG. The sub-
1548 team's membership, meeting schedule, and meeting minutes are found on the RAPWG web site.

1549

1550 8.2.1 ICANN Agreement Landscape:

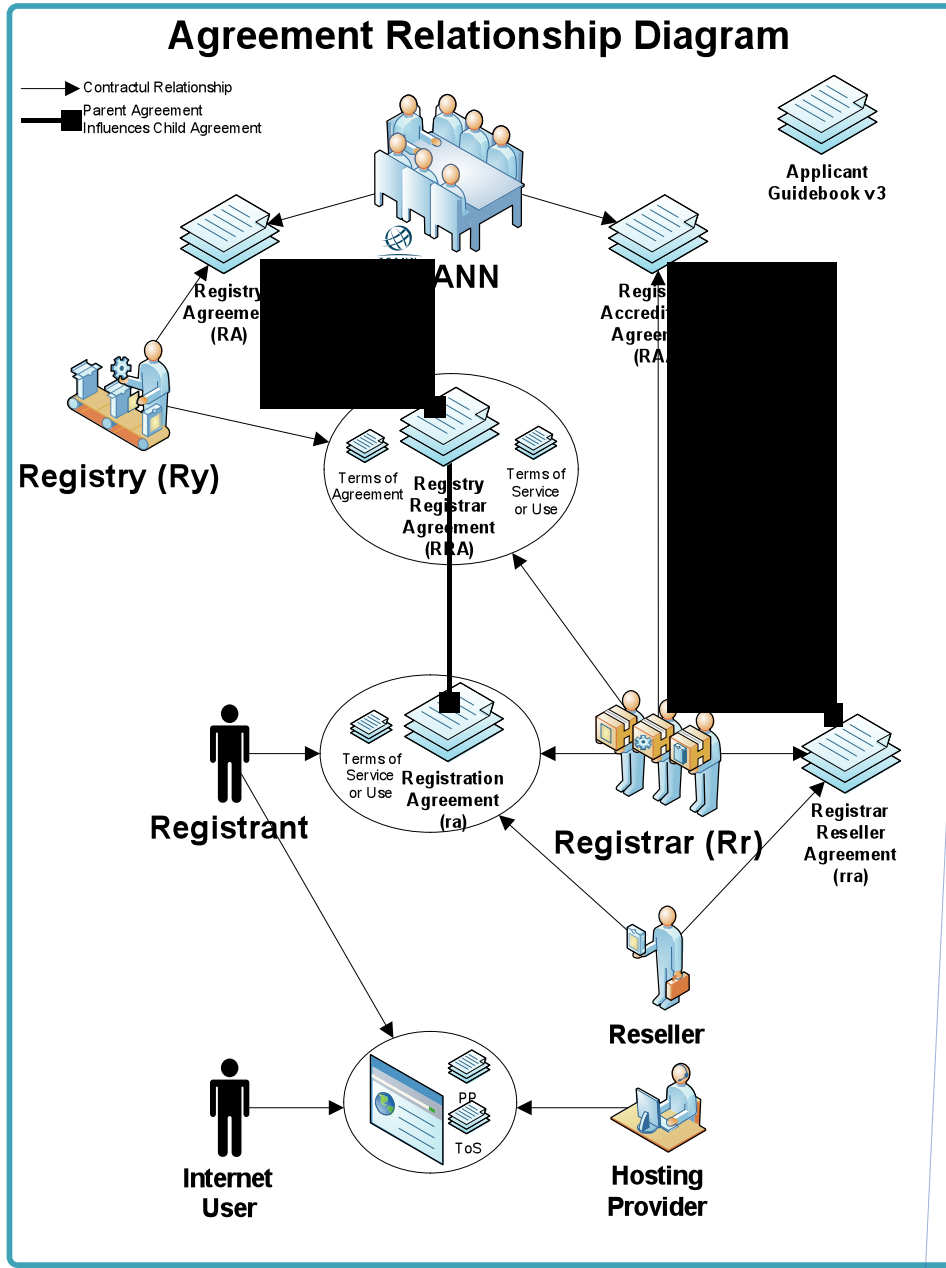
1551 The following diagram is meant to define scope and visually represent the relationships
1552 between parties and the contracts that bind them. Additionally, nested relationships between
1553 the agreements themselves are depicted.

1554

1555 Market Participants:

- 1556 • ICANN
- 1557 • Registry (Ry)
- 1558 • Registrar (Rr)

- 1559 • Registrant
- 1560 • Hosting Provider
- 1561 • Internet User
- 1562
- 1563 Agreements:
- 1564 • Registry Agreement (RA)
- 1565 • Registry Registrar Agreement (RRA)
- 1566 • Registrar Accreditation Agreement (RAA)
- 1567 • Registration Agreement (ra)
- 1568 • Registrar Reseller Agreement (rra)**
- 1569 • Terms of Service**
- 1570 • Terms of Use**
- 1571 • Terms of Agreement**
- 1572 **Agreements typically not in scope of primary dispersion research



Marika Konings 2/2/10 11:00
Deleted:

1573

1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603

8.2.2 Dispersion Research

Registry Agreement (RA) Dispersion:

[Refer to the GNSO Issues Report on Registration Abuse Policies](#)

[Section 4 - Provisions in Registry Agreements relating to abuse](#)

[Pages 11 - 29](#)

<http://gns0.icann.org/files/gns0/issues/registration-abuse/gns0-issues-report-registration-abuse-policies-29oct08.pdf>

Registry Registrar Agreement (RRA) Dispersion:

[Refer to the GNSO Issues Report on Registration Abuse Policies](#)

[Section 4 - Provisions in Registry Agreements relating to abuse](#)

[Pages 11 - 29](#)

<http://gns0.icann.org/files/gns0/issues/registration-abuse/gns0-issues-report-registration-abuse-policies-29oct08.pdf>

[RRA Templates are contained within the RA and hence the analysis is combined with appendix 1.](#)

Registrar Accreditation Agreement (RAA) Dispersion:

[Because the RAA is template driven, a quick inventory of Registration Abuse Types \(as defined by the RAPWG\) was conducted within the RAA template instead of a formal dispersion study.](#)

[Two RAAs exist. A version from May 2001 existed until the most recent May 2009 version was released. With over 80+% adoption rates by Registrars to the May 2009 version, it was the only](#)

[RAA reviewed for dispersion.](#)

<http://www.icann.org/en/registrar/agreements.html>

Marika Konings 2/2/10 10:59
Deleted: Findings
Marika Konings 2/2/10 10:59
Deleted: :

1604 [The May 2009 RAA does contain provisions that align with abuse types defined by the Working](#)
1605 [Group. These include WhoIS, UDRP, and Privacy language. However, the latest RAA does not](#)
1606 [contain any language relative to take-down, conduct & use, abuse definitions, and](#)
1607 [indemnification to protect parties from taking action against abuse.](#)

1608
1609 [In parallel to the RAPWG, a Working Group to enhance the RAA is underway. It is the UoC's](#)
1610 [intent to share any recommendations that appear to align with RAA WG actions. Based on the](#)
1611 [latest presentations from ICANN Seoul, WG members have already identified gaps around](#)
1612 [Malicious Conduct, Cybersquatting, Privacy/Proxy Services, and complete information disclosure](#)
1613 [with Affiliates & Resellers.](#)

1614
1615 **[Registration Agreement \(ra\) Dispersion:](#)**

1616
1617 [Refer to the GNSO Issues Report on Registration Abuse Policies](#)
1618 [Section 5 - Provisions in Registration Agreements relating to abuse](#)
1619 [Pages 30 - 37](#)

1620 <http://gnso.icann.org/files/gnso/issues/registration-abuse/gnso-issues-report-registration->
1621 [abuse-policies-29oct08.pdf](http://gnso.icann.org/files/gnso/issues/registration-abuse/gnso-issues-report-registration-)

1622
1623 **[Registration Agreement \(ra\) Dispersion Study](#)**

1624
1625 [An evaluation of publicly available online agreements \(Domain Registration Agreement,](#)
1626 [Universal Terms of Service, etc..\), from a representative sample of registrars was performed to](#)
1627 [determine the degree of variation among agreement provisions relative to abuse. This](#)
1628 [evaluation, essentially, is an inventory of sections within the registration agreement. It attempts](#)
1629 [to quantify "current state" for the purpose of providing a visual representation of dispersion.](#)

1630
1631 [By review of the various registration agreements, sections began to naturally form in to forty or](#)
1632 [so categories in which the registration agreements could be inventoried. For each of the 22](#)
1633 [Registrars, from the representative pool, an Excel spreadsheet was used to track the binary](#)

1634 [existence of each agreement category. If a category was found, the spreadsheet would be](#)
1635 [incremented accordingly, and if the section was relevant to abuse, the corresponding](#)
1636 [agreement language was pasted in to the spreadsheet. If no section was found, the category](#)
1637 [requirement was not met, nor was it incremented.](#)

1638
1639 [It should be noted, that this was not a compliance exercise, and as such, all results shared are](#)
1640 [anonymous. The representative sample of registrars is based on % market share of held](#)
1641 [registrations per webhosting.info as of June 2009. Within that sample, a general guiding](#)
1642 [principle for selection of the 22 registrars was the top, middle, and bottom market participants.](#)
1643 [This sample of 22 Registrars makes up approximately 59% of total market share. Additionally,](#)
1644 [the sample also attempts to gain representation across varying countries.](#)

1645
1646 [The actual spreadsheet and presentation reports can be found at the UoC Wiki Attachments](#)
1647 [section:](#)

1648 https://st.icann.org/reg-abuse-wg/index.cgi?uniformity_sub_team

1649 [RAPWG-UofC Dispersion Matrix 09152009.xls](#)

1650 [RAPWG-UofC Report 09152009.pdf](#)

1651
1652 [The diagram here shows a screen shot of a Registration Agreement \(ra\) on the left. Each red](#)
1653 [arrow points to a defined section within the agreement. On the right side of the diagram are the](#)
1654 [categories that formed from the inventory. Those labeled in the blue boxes pertain to the abuse](#)
1655 [types within scope of the RAPWG.](#)

1656

The screenshot shows a document titled "Domain Name Registration Agreement" with several sections: 1. AGREEMENT, 2. SELECTION OF A DOMAIN NAME, 3. FEES, 4. TERM, 5. MODIFICATIONS TO AGREEMENT, and 6. MODIFICATIONS TO YOUR ACCOUNT. Red arrows from the text in these sections point to a central label "Agreement Sections". To the right of this label is a table titled "RAP Categories" with the following rows: UDRP, Termination of Service, Restriction of Service / Takedown / Revocation, Registrar Transfer Dispute Resolution Policy, Contact Information, Conduct & Use, Spam, Renewals, and Expiration. Further to the right is a list titled "Other Categories" containing various items such as 3rd Party, Account Access, Agency, Agree to Agreement, Breach, Fees & Payment, Force Majeure, Guaranty, Indemnification, Infancy, Language, Law & Jurisdiction, License to Registrar, Limitation of Liability, Modifications / Passage of T, Non-waiver, Notices / Announcements, Ownership, Parked Services, Representation & Warranty, Reseller or Licensor, Right of Refusal, Services / Responsibilities, Severability, Survival, Terms / Parties, Transfers, Use of Information (privacy), User/Client Responsibilities, Representations, & Warrant, Waiver, Misc. Notes (flag not count cc or gTLD Specific Sections).

1657
1658
1659
1660
1661
1662
1663
1664

[This screen shot represents the entire spreadsheet used to inventory Registration Agreement sections across the 22 Registrars. The zoom here is at 10%. This screen shot also includes those categories not relevant to abuse, and as such will not show pasted language from the agreement:](#)

1665

| Section | Item | Description | Policy | Impact | Recommendation | Timeline | Responsible Party | Status | Notes |
|-----------|------|-------------|---------------|---------------|-----------------------|-----------------|--------------------------|---------------|--------------|
| Section 1 | 1.1 | Item 1.1.1 | Policy 1.1.1 | Impact 1.1.1 | Recommendation 1.1.1 | Timeline 1.1.1 | Responsible Party 1.1.1 | Status 1.1.1 | Notes 1.1.1 |
| | 1.2 | Item 1.2.1 | Policy 1.2.1 | Impact 1.2.1 | Recommendation 1.2.1 | Timeline 1.2.1 | Responsible Party 1.2.1 | Status 1.2.1 | Notes 1.2.1 |
| | 1.3 | Item 1.3.1 | Policy 1.3.1 | Impact 1.3.1 | Recommendation 1.3.1 | Timeline 1.3.1 | Responsible Party 1.3.1 | Status 1.3.1 | Notes 1.3.1 |
| | 1.4 | Item 1.4.1 | Policy 1.4.1 | Impact 1.4.1 | Recommendation 1.4.1 | Timeline 1.4.1 | Responsible Party 1.4.1 | Status 1.4.1 | Notes 1.4.1 |
| | 1.5 | Item 1.5.1 | Policy 1.5.1 | Impact 1.5.1 | Recommendation 1.5.1 | Timeline 1.5.1 | Responsible Party 1.5.1 | Status 1.5.1 | Notes 1.5.1 |
| | 1.6 | Item 1.6.1 | Policy 1.6.1 | Impact 1.6.1 | Recommendation 1.6.1 | Timeline 1.6.1 | Responsible Party 1.6.1 | Status 1.6.1 | Notes 1.6.1 |
| | 1.7 | Item 1.7.1 | Policy 1.7.1 | Impact 1.7.1 | Recommendation 1.7.1 | Timeline 1.7.1 | Responsible Party 1.7.1 | Status 1.7.1 | Notes 1.7.1 |
| | 1.8 | Item 1.8.1 | Policy 1.8.1 | Impact 1.8.1 | Recommendation 1.8.1 | Timeline 1.8.1 | Responsible Party 1.8.1 | Status 1.8.1 | Notes 1.8.1 |
| | 1.9 | Item 1.9.1 | Policy 1.9.1 | Impact 1.9.1 | Recommendation 1.9.1 | Timeline 1.9.1 | Responsible Party 1.9.1 | Status 1.9.1 | Notes 1.9.1 |
| | 1.10 | Item 1.10.1 | Policy 1.10.1 | Impact 1.10.1 | Recommendation 1.10.1 | Timeline 1.10.1 | Responsible Party 1.10.1 | Status 1.10.1 | Notes 1.10.1 |
| Section 2 | 2.1 | Item 2.1.1 | Policy 2.1.1 | Impact 2.1.1 | Recommendation 2.1.1 | Timeline 2.1.1 | Responsible Party 2.1.1 | Status 2.1.1 | Notes 2.1.1 |
| | 2.2 | Item 2.2.1 | Policy 2.2.1 | Impact 2.2.1 | Recommendation 2.2.1 | Timeline 2.2.1 | Responsible Party 2.2.1 | Status 2.2.1 | Notes 2.2.1 |
| | 2.3 | Item 2.3.1 | Policy 2.3.1 | Impact 2.3.1 | Recommendation 2.3.1 | Timeline 2.3.1 | Responsible Party 2.3.1 | Status 2.3.1 | Notes 2.3.1 |
| | 2.4 | Item 2.4.1 | Policy 2.4.1 | Impact 2.4.1 | Recommendation 2.4.1 | Timeline 2.4.1 | Responsible Party 2.4.1 | Status 2.4.1 | Notes 2.4.1 |
| | 2.5 | Item 2.5.1 | Policy 2.5.1 | Impact 2.5.1 | Recommendation 2.5.1 | Timeline 2.5.1 | Responsible Party 2.5.1 | Status 2.5.1 | Notes 2.5.1 |
| | 2.6 | Item 2.6.1 | Policy 2.6.1 | Impact 2.6.1 | Recommendation 2.6.1 | Timeline 2.6.1 | Responsible Party 2.6.1 | Status 2.6.1 | Notes 2.6.1 |
| | 2.7 | Item 2.7.1 | Policy 2.7.1 | Impact 2.7.1 | Recommendation 2.7.1 | Timeline 2.7.1 | Responsible Party 2.7.1 | Status 2.7.1 | Notes 2.7.1 |
| | 2.8 | Item 2.8.1 | Policy 2.8.1 | Impact 2.8.1 | Recommendation 2.8.1 | Timeline 2.8.1 | Responsible Party 2.8.1 | Status 2.8.1 | Notes 2.8.1 |
| | 2.9 | Item 2.9.1 | Policy 2.9.1 | Impact 2.9.1 | Recommendation 2.9.1 | Timeline 2.9.1 | Responsible Party 2.9.1 | Status 2.9.1 | Notes 2.9.1 |
| | 2.10 | Item 2.10.1 | Policy 2.10.1 | Impact 2.10.1 | Recommendation 2.10.1 | Timeline 2.10.1 | Responsible Party 2.10.1 | Status 2.10.1 | Notes 2.10.1 |

1666

| Section | Item | Description | Policy | Impact | Recommendation | Timeline | Responsible Party | Status | Notes |
|-----------|------|-------------|---------------|---------------|-----------------------|-----------------|--------------------------|---------------|--------------|
| Section 3 | 3.1 | Item 3.1.1 | Policy 3.1.1 | Impact 3.1.1 | Recommendation 3.1.1 | Timeline 3.1.1 | Responsible Party 3.1.1 | Status 3.1.1 | Notes 3.1.1 |
| | 3.2 | Item 3.2.1 | Policy 3.2.1 | Impact 3.2.1 | Recommendation 3.2.1 | Timeline 3.2.1 | Responsible Party 3.2.1 | Status 3.2.1 | Notes 3.2.1 |
| | 3.3 | Item 3.3.1 | Policy 3.3.1 | Impact 3.3.1 | Recommendation 3.3.1 | Timeline 3.3.1 | Responsible Party 3.3.1 | Status 3.3.1 | Notes 3.3.1 |
| | 3.4 | Item 3.4.1 | Policy 3.4.1 | Impact 3.4.1 | Recommendation 3.4.1 | Timeline 3.4.1 | Responsible Party 3.4.1 | Status 3.4.1 | Notes 3.4.1 |
| | 3.5 | Item 3.5.1 | Policy 3.5.1 | Impact 3.5.1 | Recommendation 3.5.1 | Timeline 3.5.1 | Responsible Party 3.5.1 | Status 3.5.1 | Notes 3.5.1 |
| | 3.6 | Item 3.6.1 | Policy 3.6.1 | Impact 3.6.1 | Recommendation 3.6.1 | Timeline 3.6.1 | Responsible Party 3.6.1 | Status 3.6.1 | Notes 3.6.1 |
| | 3.7 | Item 3.7.1 | Policy 3.7.1 | Impact 3.7.1 | Recommendation 3.7.1 | Timeline 3.7.1 | Responsible Party 3.7.1 | Status 3.7.1 | Notes 3.7.1 |
| | 3.8 | Item 3.8.1 | Policy 3.8.1 | Impact 3.8.1 | Recommendation 3.8.1 | Timeline 3.8.1 | Responsible Party 3.8.1 | Status 3.8.1 | Notes 3.8.1 |
| | 3.9 | Item 3.9.1 | Policy 3.9.1 | Impact 3.9.1 | Recommendation 3.9.1 | Timeline 3.9.1 | Responsible Party 3.9.1 | Status 3.9.1 | Notes 3.9.1 |
| | 3.10 | Item 3.10.1 | Policy 3.10.1 | Impact 3.10.1 | Recommendation 3.10.1 | Timeline 3.10.1 | Responsible Party 3.10.1 | Status 3.10.1 | Notes 3.10.1 |
| Section 4 | 4.1 | Item 4.1.1 | Policy 4.1.1 | Impact 4.1.1 | Recommendation 4.1.1 | Timeline 4.1.1 | Responsible Party 4.1.1 | Status 4.1.1 | Notes 4.1.1 |
| | 4.2 | Item 4.2.1 | Policy 4.2.1 | Impact 4.2.1 | Recommendation 4.2.1 | Timeline 4.2.1 | Responsible Party 4.2.1 | Status 4.2.1 | Notes 4.2.1 |
| | 4.3 | Item 4.3.1 | Policy 4.3.1 | Impact 4.3.1 | Recommendation 4.3.1 | Timeline 4.3.1 | Responsible Party 4.3.1 | Status 4.3.1 | Notes 4.3.1 |
| | 4.4 | Item 4.4.1 | Policy 4.4.1 | Impact 4.4.1 | Recommendation 4.4.1 | Timeline 4.4.1 | Responsible Party 4.4.1 | Status 4.4.1 | Notes 4.4.1 |
| | 4.5 | Item 4.5.1 | Policy 4.5.1 | Impact 4.5.1 | Recommendation 4.5.1 | Timeline 4.5.1 | Responsible Party 4.5.1 | Status 4.5.1 | Notes 4.5.1 |
| | 4.6 | Item 4.6.1 | Policy 4.6.1 | Impact 4.6.1 | Recommendation 4.6.1 | Timeline 4.6.1 | Responsible Party 4.6.1 | Status 4.6.1 | Notes 4.6.1 |
| | 4.7 | Item 4.7.1 | Policy 4.7.1 | Impact 4.7.1 | Recommendation 4.7.1 | Timeline 4.7.1 | Responsible Party 4.7.1 | Status 4.7.1 | Notes 4.7.1 |
| | 4.8 | Item 4.8.1 | Policy 4.8.1 | Impact 4.8.1 | Recommendation 4.8.1 | Timeline 4.8.1 | Responsible Party 4.8.1 | Status 4.8.1 | Notes 4.8.1 |
| | 4.9 | Item 4.9.1 | Policy 4.9.1 | Impact 4.9.1 | Recommendation 4.9.1 | Timeline 4.9.1 | Responsible Party 4.9.1 | Status 4.9.1 | Notes 4.9.1 |
| | 4.10 | Item 4.10.1 | Policy 4.10.1 | Impact 4.10.1 | Recommendation 4.10.1 | Timeline 4.10.1 | Responsible Party 4.10.1 | Status 4.10.1 | Notes 4.10.1 |

1667

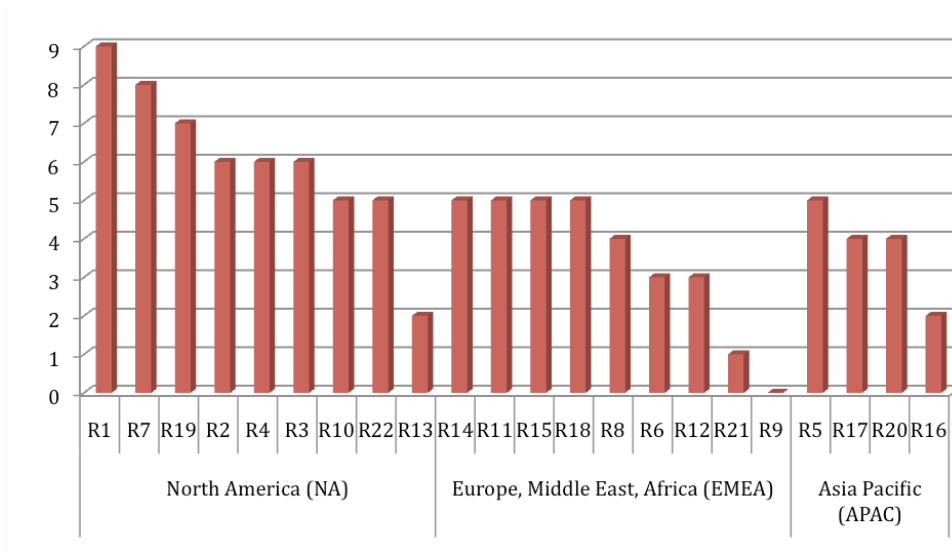
1668 This screen shot represents a summary view of the previous spreadsheet. The legend is
 1669 listed below, but basically the variance between the green and yellow coloring depicts the
 1670 dispersion found within agreements relative to abuse. The gray section to the right provides
 1671 "hit rate" percentages of agreement sections by region and overall. Please refer the UoC
 1672 Wiki for the actual reports to zoom in and gain a clearer understanding.
 1673

Legend:

- 1 Agreement met category requirement by formal section definition
- 0 Category requirement flagged via separate agreement
- Formal section definition of category not found within agreement
- Tier 2 or 3 Agreement not found or not in scope

1674
 1675
 1676
 1677 The chart below provides a different view at the dispersion across Registration Agreements. The
 1678 Y Axis represents the number of categories where the agreement satisfied the formal section

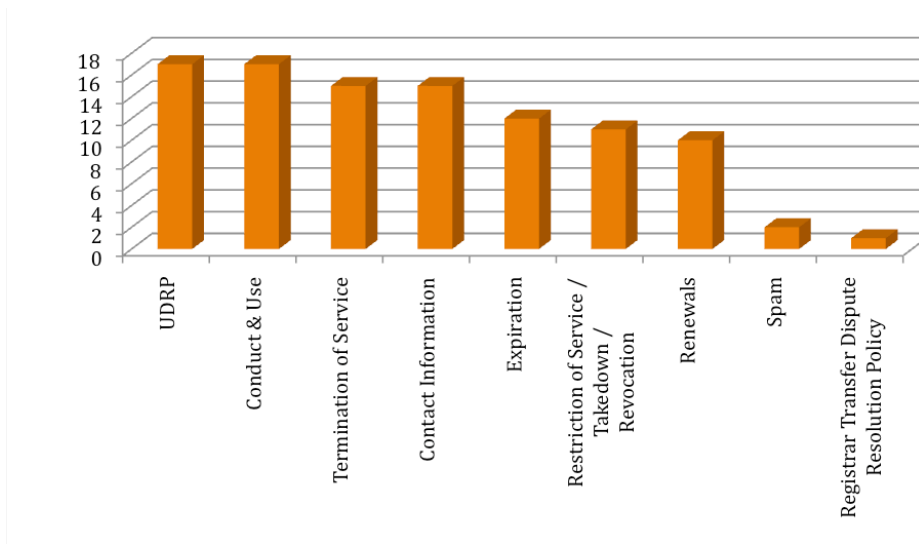
1679 [definition requirements while the X Axis represents registrars by region, sorted highest to least](#)
1680 [\(left to right\).](#)



1681

1682

1683 [This chart represents categories with the greatest achievement of section definition.](#)



1684

1685

1686 | **8.2.3 Dispersion & Consistency**

1687

1688 | The UoC sub-team believed that uniformity does not exist among “RA, RRA, RAA and ra”
1689 | agreements relative to abuse provisions. The sub-team was of the belief that increased
1690 | uniformity is important for the marketplace and helps promote equal competition, and that
1691 | while perfect uniformity is not realistic, it should be striven for when and where feasible.

1692

1693 | At the same time, the team also recognized that lack of uniformity complicates efforts to
1694 | mitigate abusive uses of domains, but is not a predicate for abuse that we see today, and that if
1695 | policies are consistent, then greater responsibility to enforce the policy consistently falls upon
1696 | ICANN.

1697

1698 | **8.2.4 Registration Abuse Provision Baseline**

1699 | - The sub-team agreed that if any sort of uniformity in agreements is to be implemented,
1700 | a minimal baseline of provision or language would be the best method to accommodate
1701 | the various business models.

1702 | - The sub-team thought that a lowest common denominator (minimum requirement)
1703 | approach with abuse provisions is best and allows market participants to not be
1704 | constrained by exceeding minimums in efforts to promote differentiation within the
1705 | competitive landscape.

- 1706 | o The sub-team recognized the spectrum of abuse provisions can range from:
- 1707 | ▪ General language with broad powers to act against all kinds of abuse, or
 - 1708 | ▪ Specific language which can be limiting; and may not be adaptive to
1709 | changing conditions
- 1710 | o Finding the right balance of language that provides adequate authority to
1711 | respond to abuse with adequate protection from lawsuits is required.

Marika Konings 2/2/10 10:59
Deleted: Code ... [4]
- 1/2/10 13:14
Formatted: Bullets and Numbering
Marika Konings 2/2/10 11:08
Formatted: Font color: Black
Marika Konings 2/2/10 11:09
Formatted: Underline, Font color: Black
- 1/2/10 15:41
Formatted: No underline

Marika Konings 2/2/10 11:05
Deleted: Abuse Provision Baseline
Marika Konings 2/2/10 20:07
Deleted: (APB)

- 1712 o A “One size fits all” kind of provision that can anticipate future or unknown
1713 abuses was the sub-team’s desire, but equally recognize the existence of varying
1714 models prevent this notion.
- 1715 - The sub-team thought that any provision baseline should be clearly communicated and
1716 shared with market participants and that high degrees of transparency is required
1717 where participants choose to exceed any baselines or minimums that are established.
- 1718 - The sub-team agreed that outcomes from any future and not-yet-determined
1719 registration abuse policies PDP will be long coming and that in the meantime it would be
1720 a useful thing for ICANN, Registries, and Registrars to develop abuse provisions and/or
1721 continue to enhance abuse provisions for their agreements with continued voluntary,
1722 proactive enforcement as necessary. Additionally, the sub-team agreed that the
1723 investigation and deployment of best practices would be a great interim step until such
1724 a PDP is complete.

Marika Konings 2/2/10 11:21

Deleted: “

Marika Konings 2/2/10 11:21

Deleted: d model,”

Marika Konings 2/2/10 11:22

Deleted: the sub-team team did not recognize variance among business types

- 1/2/10 15:41

Deleted:

Marika Konings 2/2/10 11:09

Deleted: APB

- 1/2/10 15:42

Deleted: A

- 1/2/10 15:42

Deleted: ,

1726 8.2.5 Sub-Team Conclusions & Guiding Principles

1727 Over the course of UoC sub-team meetings and research findings, reoccurring themes
1728 developed with consistent agreement leading to sub-team consensus and defined boundaries
1729 for recommendations that the sub-team created.

Marika Konings 2/2/10 11:09

Formatted: Bullets and Numbering

1732 8.2.6 RAPWG Discussion of Sub-Team Work

1733 The members of the sub-team reported their results to the whole RAPWG team for review.

1734 When the wider RAPWG discussed the sub-team’s analysis, there was not agreement about the
1735 sub-team’s findings and recommendations.

1736 Some RAPWG members believed that uniformity already exists in the important and relevant
1737 ways. Observations included:

- 1738 • Registries, registrars, and registrants are required to follow Consensus Policies. So, if
1739 there is a registration abuse, ICANN can make consensus policy about that abuse, and
1740

Marika Konings 2/2/10 11:10

Formatted: Font color: Black

Marika Konings 2/2/10 11:11

Formatted: Bullets and Numbering

- 1/2/10 16:35

Formatted: Font:Calibri, 11 pt

- 1/2/10 14:16

Deleted: and

- 1742 the resulting policy will be applied to all contracted parties. The Consensus Policy
1743 process is a mechanism specifically designed to create uniformity where it is needed,
1744 and it guarantees uniformity.
- 1745 • All registrars are bound to a uniform RAA. While two version of the RAA currently exist,
1746 the great majority of the registered gTLD domains are now covered under the new
1747 (2009) RAA, and the old RAA (2001) is being phased out in a planned fashion.
 - 1748 • Language in the RAA requires registrars and registrants to adhere to all ICANN policies.
 - 1749 • Some amount of non-uniformity is necessary. For example, sTLDs may require language
1750 in their contracts to define their unique sponsorship and eligibility needs.
 - 1751 • Uniformity for the sake of uniformity does not necessarily solve any problem.

1753 The sub-team advocated the exploration of “general language with broad powers to act
1754 against all kinds of abuse,” and provisions “that can anticipate future or unknown abuses.”
1755 Some RAPWG members expressed concern that these ideas might not be desirable or
1756 realistic. They might be a solution in search of an undefined problem, and might not
1757 include adequate consideration of who is being harmed, how, and to what extent. The
1758 RAPWG agreed in its definitional work that “The party or parties harmed, and the substance
1759 or severity of the abuse, should be identified and discussed in relation to a specific proposed
1760 abuse.” Members expressed that it is difficult to anticipate future or unknown abuses, and
1761 raised the issue that general and/or pre-emptive policies may create collateral damage and
1762 harm registrants or other parties in unexpected fashions. In general, the RAPWG discussed
1763 how in the past consensus policy-making efforts, specific registration abuses were verified
1764 and understood, and then specific policies and procedures were designed to address them.

1765
1766 Some members were of the opinion that the sub-team did not always distinguish adequately in
1767 its contracts analysis between registration abuse provisions and provisions designed to address
1768 malicious uses of domains. This distinction can be critical for policy-making.

1769
1770 Regarding uniformity of registrar-registrant agreements and TLD-specific terms of service:
1771 Registrars do have the right to set their terms of service as long as they are consistent with

- 1/2/10 16:52
Deleted: Some RAPWG members expressed that a general APB may not be a realistic goal. A concern is

- 1/2/10 16:51
Formatted: Indent: Left: 0,25"

- 1/2/10 16:45
Deleted: that

- 1/2/10 16:56
Deleted: creation

- 1/2/10 16:45
Deleted: "

Marika Konings 2/2/10 11:18
Deleted: -

1772 ICANN requirements. Similarly, many registries have the contractual right to institute policies
1773 and procedures for their own TLDs, and it was unclear to some RAPWG members whether ABPs
1774 would alter those existing contractual rights. As per the exploration of malicious use above,
1775 ICANN does not appear to have the ability to force registrars and registries to implement
1776 domain suspensions for malicious use alone.

1777
1778 There was some disagreement with the sub-team’s statement that “uniformity is important for
1779 the marketplace and helps promote equal competition;” RAPWG members commented that
1780 contractual variances in registrar-registrant agreements are a way that registrars differentiate
1781 themselves in the market, and can help registrars adhere to the laws of the jurisdictions in
1782 which they are incorporated or operate.

1783

1784 **8.3 Recommendations**

1785

1786 **RECOMMENDATION:** The RAPWG recommends the creation of an Issues Report to evaluate
1787 whether a minimum baseline of registration abuse provisions should be created for all in-scope
1788 ICANN agreements, and if created, how such language would be structured to address the most
1789 common forms of registration abuse.

1790

1791 **ALTERNATE VIEW:** [Oppose the recommendation for an Issues Report, for the following reasons:](#)

- 1792 • [All registries, registrars, and registrants are already contractually obligated to abide by](#)
1793 [ICANN policies, notably Consensus Policies.](#)
- 1794 • [The Consensus Policy process is a mechanism specifically designed to create uniformity](#)
1795 [where it is needed.](#)
- 1796 • [Consensus Policies or contractual provisions should be created to solve specific](#)
1797 [problems, after the abuse’s scope and impact are understood. General and/or pre-](#)
1798 [emptive policies may create collateral damage and harm registrants or other parties in](#)
1799 [unexpected fashions.](#)
- 1800 • [Uniformity for the sake of uniformity is not a solution to any identified problem. The](#)
1801 [supporters of an Issues Report did not identify why “a minimum baseline of registration](#)

- 1/2/10 14:04

Deleted:

1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812

abuse provisions” is needed, or whether such might better curtail or address any problem. It is unclear what purpose might be served by continuing down that proposed path.

- It may not be desirable or possible to create a baseline applicable to diverse entities. Some amount of non-uniformity is necessary. Contracted parties should also have some rights to create their own policies as long as they do not conflict with ICANN policies.

- 1/2/10 14:27
Deleted: -

- 1/2/10 15:48

Deleted:

1812 9. Meta-Issues

1813 The RAPWG identified registration abuse “meta-issues.” These meta-issues have a number of
1814 attributes in common:

1815

- 1816 • They are being discussed in various Working Groups and Advisory Groups
- 1817 simultaneously.
- 1818 • Their scope spans a number of ICANN policies
- 1819 • Previous groups have discussed these issues without satisfactory resolution
- 1820 • They are worthy of substantive discussion and action, but may not lend themselves to
- 1821 resolution through current policy processes

1822

1823 9.1 Meta-issue : Uniformity of reporting

1824

1825 This working group has identified the need for more uniformity in the mechanisms to initiate,
1826 track, and analyze policy-violation reports. The IRTP Working Group identified a similar need
1827 during its review of compliance reports in that arena. This issue is much broader than
1828 registration abuse, is being discussed by a number of working and advisory groups
1829 simultaneously, and will require more than simple uniformity of contracts to address.

1830

1831 9.1.1 The Problem

1832

1833 The processes by which a person experiencing a problem learns about their options to resolve
1834 that problem, or learns which remedies are covered by ICANN policy and which are not, is
1835 sometimes difficult. As a result:

1836

- 1837 • End-users and registrants find it confusing and difficult to identify the most appropriate
- 1838 problem-reporting venue or action to take when they experience problems.

- 1839 • Registrars and registries are frustrated if their customers file complaints in error, in the
1840 wrong place, or without first seeking help from the most relevant provider.
1841 • Working and advisory groups find their work hampered by the lack of reliable (rather
1842 than anecdotal) data upon which to base policy decisions.

1843

1844 In addition, the process of reporting a perceived policy violation could be used to educate
1845 people on the limits of ICANN policies and available options if their issue is not covered by
1846 policy.

1847

1848 The RAPWG suggests, as a starting point for discussion, that every abuse policy should have:

- 1849 • **Reporting:** a mechanism whereby violations of the policy can be reported by those who
1850 are impacted
- 1851 • **Notification:** standards as to how contracted parties make visible:
- 1852 ○ where to report policy violations,
 - 1853 ○ “plain language” definitions of what constitutes a “reportable” problem,
 - 1854 ○ “just in time education” describing reporting or action options that are available
1855 when the person’s problem falls outside ICANN policy.
- 1856 • **Tracking:** transparent processes to collect, analyze, and publish summaries of valid
1857 policy-violation reports, the root-causes of the problems and their final disposition
- 1858 • **Compliance:** processes to provide due process, and sanctions that will be applied, in the
1859 case of policy violations.

1860

1861 [If the GNSO creates a subsequent effort to address this issue, it might consider the following](#)
1862 [tentative list of goals:](#)

1863

- 1864 • [Providing “just in time” education and knowledge to people wanting to report problems](#)
- 1865 • [Making it easier to submit a valid complaint](#)
- 1866 • [Reduce the number of erroneous complaints](#)
- 1867 • [Improving understanding of the limits of ICANN policies and other options to pursue if](#)
1868 [the issue is not covered by policy](#)

- 1869 • [Improving the effectiveness of policy-compliance activities](#)
- 1870 • [Improving the data available for GNSO \(working-group\) and ICANN \(advisory-group\)](#)
- 1871 [policy-making](#)
- 1872 • [Improving the data available for compliance activities](#)
- 1873 • [Answering the question “which comes first, policy-process or definitive data describing](#)
- 1874 [the problem?” along with suggestions as to how data can be gathered when it hasn't yet](#)
- 1875 [been included in the reporting process.](#)
- 1876

1877 9.1.2 Recommendation

1878
1879 [The RAPWG recommends that the GNSO, and the larger ICANN community in general, create](#)
1880 [and support uniform reporting processes.](#)

1881 9.2 Meta-issue: Collection and Dissemination of Best Practices

1882
1883
1884 The RAPWG has identified the need for and benefit of creating and disseminating “best
1885 practices” related to aspects of domain name registration and management, for the appropriate
1886 members of the ICANN community. Best practices should also be kept current and relevant.

1887 The question is how ICANN can support such efforts in a structured way.

1888
1889 This recommendation is a “meta-issue” because it is much broader than registration abuse, is
1890 being discussed by a number of working and advisory groups simultaneously, and has potential
1891 impact for almost any current and future working or advisory group.

1893 9.2.1 Definition of “Best Practices”

1894
1895 From Wikipedia (http://en.wikipedia.org/wiki/Best_practices):
1896

- 1/2/10 16:10

Deleted: The RAPWG suggests that this “meta-issue” be addressed either by a PDP working group, a best-practices working group or an ICANN advisory group, with the goals of: -
-
<#>Providing “just in time” education and knowledge to people wanting to report problems -
<#>Making it easier to submit a valid complaint -
<#>Reduce the number of erroneous complaints -
<#>Improving understanding of the limits of ICANN policies and other options to pursue if the issue is not covered by policy -
<#>Improving the effectiveness of policy-compliance activities -
<#>Improving the data available for GNSO (working-group) and ICANN (advisory-group) policy-making -
<#>Improving the data available for compliance activities -
<#>Answering the question “which comes first, policy-process or definitive data describing the problem?” along with suggestions as to how data can be gathered when it hasn't yet been included in the reporting process. -

1897 *A best practice is a technique, method, process, activity, incentive, or reward that is*
1898 *believed to be more effective at delivering a particular outcome than any other*
1899 *technique, method, process, etc. when applied to a particular condition or circumstance.*
1900 *The idea is that with proper processes, checks, and testing, a desired outcome can be*
1901 *delivered with fewer problems and unforeseen complications. Best practices can also be*
1902 *defined as the most efficient (least amount of effort) and effective (best results) way of*
1903 *accomplishing a task, based on repeatable procedures that have proven themselves over*
1904 *time for large numbers of people.*

1905
1906 *A given best practice is only applicable to particular condition or circumstance and may*
1907 *have to be modified or adapted for similar circumstances. In addition, a "best" practice*
1908 *can evolve to become better as improvements are discovered.*

1909
1910 The members of the RAPWG discussed that “best practices” should be considered non-binding
1911 by definition, and should therefore not have an implication of finality, obedience, or
1912 universality. This distinguishes them from binding requirements such as Consensus Policies and
1913 contractual obligations, which are considered final and require compliance, and are created via
1914 other processes at ICANN. Best practices may often be a good alternative when binding
1915 requirements are not applicable or appropriate. (In a parallel example, IETF Best Practices or
1916 “best current practice RFCs” are recommendations only, and the IETF chose not to make them
1917 Internet Standards for a reason.) Best practices are also flexible, can be updated as needed, and
1918 can be adopted and adapted by various users according to their varying needs. As has been
1919 noted in this paper, that is helpful because industry parties often face very different problems,
1920 to different degrees, etc.

1921 1922 **9.2.2 Background**

1923
1924 A number of working and advisory groups are coming up with many good ideas for addressing a
1925 wide variety of problems in the industry. The group’s participants often label these ideas as
1926 “best practices”. However, many of these ideas do not lend themselves well to crafting as

1927 policy, for policies are often narrow in scope, limited in the time they could be effective, or
1928 difficult to capture as policy concepts or contract terms. This is particularly true in the areas
1929 surrounding malicious use. Yet all industry participants could benefit greatly by adopting many
1930 of these best practices. Unfortunately, no formal mechanisms for collecting such practices,
1931 keeping them updated, or disseminating them to all relevant industry participants exists today
1932 within the ICANN community. Thus, much of the good work done in these groups is not
1933 captured effectively if it is not included in their policy-making outcomes.

1934
1935 Best practices in the field of anti-abuse or security often lose their effectiveness in a relatively
1936 short amount of time. This does not lend well to formal policy, but sharing effective techniques
1937 with peers in the field can still be very beneficial.

1938
1939 Best practices in the field of anti-abuse or security are often very sensitive, and industry
1940 participants would not always like some of them made public so that bad actors can learn from
1941 them and adapt new tactics. How can sensitive best practices be safely disseminated to industry
1942 participants? How can the veracity of all industry participants be assured as well?

1943
1944 [If the GNSO creates a subsequent effort to address this issue, it might consider the following](#)
1945 [tentative list of goals:](#)

- 1946 • [Creating mechanisms within the ICANN community to support the creation and](#)
1947 [maintenance of best practices efforts in a structured way.](#)
- 1948 • [Creating multiple channels \(some private or secure\) for dissemination of best practices](#)
1949 [to all relevant community members.](#)
- 1950 • [Incorporating the gathering and recommendation of best practices into the processes](#)
1951 [used by various policy and advisory working groups.](#)
- 1952 • [Instituting practices to measure and incentivize adoption of best practices across the](#)
1953 [industry.](#)
- 1954 • [Launching regular review processes where universal best practices might be](#)
1955 [incorporated into more formal policies, when appropriate.](#)

1956

- 1/2/10 16:15

Deleted: <#> .

1957 **9.2.3 Recommendation**

1958

1959 [The RAPWG recommends that the GNSO, and the larger ICANN community in general, create](#)
1960 [and support structured, funded mechanisms for the collection and maintenance of best](#)
1961 [practices.](#)

1962

- 1/2/10 13:29

Deleted: The working group suggests that this "meta-issue" be addressed either by a PDP working group or an ICANN advisory group, with the goals of:

-
- <#>Creating mechanisms within the ICANN community to support the creation and maintenance of best practices efforts in a structured way. -
- <#>Creating multiple channels (some private or secure) for dissemination of best practices to all relevant community members. -
- <#>Incorporating the gathering and recommendation of best practices into the processes used by various policy and advisory working groups. -
- <#>Instituting practices to measure and incentivize adoption of best practices across the industry. -
- <#>Launching regular review processes where universal best practices may be incorporated into more formal policies. -

1962 **10. Conclusions, Recommendations, & Next Steps**

1963

1964 [TBD]

1965

1965 **Annex I – Working Group Charter**

1966

1967 Whereas GNSO Council Resolution (20081218-3) dated December 18, 2008 called for the
1968 creation of a drafting team “to create a proposed charter for a working group to investigate the
1969 open issues documented in the issues report on Registrations[sic] Abuse Policy”.

1970

1971 Whereas a drafting team has formed and its members have discussed and reviewed the open
1972 issues documented in the issues report.

1973

1974 Whereas it is the view of the drafting Team that the objective of the Working Group should be
1975 to gather facts, define terms, provide the appropriate focus and definition of the policy issue(s),
1976 if any, to be addressed, in order to enable the GNSO Council to make an informed decision as to
1977 whether to launch PDP on registration abuse.

1978 Whereas the drafting team recommends that the GNSO Council charter a Working Group to (i)
1979 further define and research the issues outlined in the Registration Abuse Policies Issues Report;
1980 and (ii) take the steps outlined below. The Working Group should complete its work before a
1981 decision is taken by the GNSO Council on whether to launch a PDP.

1982

1983 The GNSO Council RESOLVES: To form a Working Group of interested stakeholders and
1984 Constituency representatives, to collaborate broadly with knowledgeable individuals and
1985 organizations, to further define and research the issues outlined in the Registration Abuse
1986 Policies Issues Report; and take the steps outlined in the Charter. The Working Group should
1987 address the issues outlined in the Charter and report back to the GNSO Council within 90 days
1988 following the end of the ICANN meeting in Mexico City.

1989

1990 **CHARTER**

1991

1992 **Scope and definition of registration abuse** – the Working Group should define domain name

1993 registration abuse, as distinct from abuse arising solely from use of a domain name while it is
1994 registered. The Working Group should also identify which aspects of the subject of registration
1995 abuse are within ICANN's mission to address and which are within the set of topics on which
1996 ICANN may establish policies that are binding on gTLD registry operators and ICANN-accredited
1997 registrars. This task should include an illustrative categorization of known abuses.

1998

1999 **Additional research and identifying concrete policy issues** – The issues report outlines a
2000 number of areas where additional research would be needed in order to understand what
2001 problems may exist in relation to registration abuse and their scope, and to fully appreciate the
2002 current practices of contracted parties, including research to:

- 2003 - 'Understand if registration abuses are occurring that might be curtailed or better
2004 addressed if consistent registration abuse policies were established'
- 2005 - 'Determine if and how [registration] abuse is dealt with in those registries [and
2006 registrars] that do not have any specific [policies] in place'
- 2007 - 'Identify how these registration abuse provisions are [...] implemented in practice or
2008 deemed effective in addressing registration abuse'.

2009

2010 In addition, additional research should be conducted to include the practices of relevant entities
2011 other than the contracted parties, such as abusers, registrants, law enforcement, service
2012 providers, and so on.

2013

2014 The Working Group should determine how this research can be conducted in a timely and
2015 efficient manner -- by the Working Group itself via a Request for Information (RFI), by obtaining
2016 expert advice, and/or by exploring other options.

2017

2018 Based on the additional research and information, the Working Group should identify and
2019 recommend specific policy issues and processes for further consideration by the GNSO Council.

2020

2021 **SSAC Participation and Collaboration:** The Working Group should (i) consider inviting a
2022 representative from the Security and Stability Advisory Committee (SSAC) to participate in the

2023 Working Group; (ii) consider in further detail the SSAC's invitation to the GNSO Council to
2024 participate in a collaborative effort on abuse contacts; and (iii) make a recommendation to the
2025 Council about this invitation.

2026

2027 **Workshop at ICANN meeting in Mexico City on Registration Abuse Policies** - In order to get
2028 broad input on and understanding of the specific nature of concerns from community
2029 stakeholders, the drafting team proposes to organize a workshop on registration abuse policies
2030 in conjunction with the ICANN meeting in Mexico City. The Working Group should review and
2031 take into account the discussions and recommendations, if any, from this workshop in its
2032 deliberations.

2033

2034 The working group established by this motion will work according to the process defined in
2035 [Working Group Processes](#).

2036

2037

2038

2038 **Annex II - The Working Group and Attendance**

2039

2040 Following the adoption of the charter by the GNSO Council, a call for volunteers was launched.

2041 The following individuals are part of the RAP WG; all have submitted Statements of Interest (see

2042 https://st.icann.org/reg-abuse-wg/index.cgi?statements_of_interest):

2043

| Name | Affiliation⁴⁹ |
|-----------------------------------|---------------------------------|
| Greg Aaron (Chair) | RySG |
| Mike Rodenbaugh (Council Liaison) | CBUC |
| James Bladel | RrSG |
| Olga Cavalli | NCA |
| Zahid Jamil | CBUC |
| Beau Brendler | ALAC |
| Jeff Neuman | RySG |
| Nacho Amadoz | RySG |
| Philip Corwin | CBUC |
| Martin Sutton | CBUC |
| Richard Tindal | RrSG |
| Greg Ogorek | CBUC |
| Faisal Shah | IPC |
| Roland Perry | Individual |
| Paul Stahura | RrSG |
| Jaime Echeverry Gomez | RrSG |
| Li Guanghao | Individual |
| Mike O'Connor | CBUC |
| Gretchen Olive | RrSG |
| Berry Cobb | CBUC |
| Jeff Eckhaus | RrSG |
| Robert Hutchinson | CBUC |
| Andy Steingruebl | Individual |

⁴⁹ RySG = Registry Stakeholdergroup, RrSG = Registrar Stakeholdergroup, CBUC = Commercial and Business Users Constituency, NCA = Nominating Committee Appointee, ALAC = At Large Advisory Committee, IPC = Intellectual Property Constituency, SSAC = Security and Stability Advisory Committee, NCUC = Non-Commercial Users Constituency

| | |
|------------------------------|------------|
| Jeremy Hitchcock | SSAC |
| Patrick Kane | RySG |
| George Kirikos ⁵⁰ | CBUC |
| Michael Young | RySG |
| Rod Rasmussen | Individual |
| Edward Nunes | NCUC |
| Frederick Felman | IPC |
| Evan Leibovitch | ALAC |
| Caleb Queern | CBUC |
| Avri Doria | NCUC |
| Chuck Gomes (GNSO Chair) | RySG |

2044

2045 [Include attendance sheet]

2046

2047

2048

Marika Konings 2/2/10 11:25
Deleted: -

Marika Konings 2/2/10 11:25
Formatted: Indent: Left: 0"

⁵⁰ Left the Working Group on [insert date]

2048

Marika Konings 2/2/10 11:24

Deleted: Annex III – Uniformity of Contracts:
Additional Background Materials -

-

Registry Agreement (RA) Dispersion: -

-

Refer to the GNSO Issues Report on Registration Abuse Policies -

Section 4 - Provisions in Registry Agreements relating to abuse -

Pages 11 - 29 -

<http://gns0.icann.org/files/gns0/issues/registration-abuse/gns0-issues-report-registration-abuse-policies-29oct08.pdf> -

-

Registry Registrar Agreement (RRA) Dispersion: -

-

Refer to the GNSO Issues Report on Registration Abuse Policies -

Section 4 - Provisions in Registry Agreements relating to abuse -

Pages 11 - 29 -

<http://gns0.icann.org/files/gns0/issues/registration-abuse/gns0-issues-report-registration-abuse-policies-29oct08.pdf> -

-

RRA Templates are contained within the RA and hence the analysis is combined with appendix 1. -

-

Registrar Accreditation Agreement (RAA)

Dispersion: -

-

Because the RAA is template driven, a quick inventory of Registration Abuse Types (as defined by the RAPWG) was conducted within the RAA template instead of a formal dispersion study. Two RAAs exist. A version from May 2001 existed until the most recent May 2009 version was released. With over 80+% adoption rates by Registrars to the May 2009 version, it was the only RAA reviewed for dispersion. -

-

<http://www.icann.org/en/registrars/agreements.html> -

-

The May 2009 RAA does contain provisions that align with abuse types defined by the Working Group. These include WhoIS, UDRP, and Privacy language. However, the latest RAA does not contain any language relative to take-down, conduct & use, abuse definitions, and indemnification to protect parties from taking action against abuse. -

-

In parallel to the RAPWG, a Working Group to enhance the RAA is underway. It is the UoC's intent to share any recommendations that appear to align with RAA WG actions. Based on the latest presentations from ICANN Seoul, WG members have already identified gaps around Malicious Conduct, Cybersquatting, Privacy/Proxy Services, and complete information disclosure with Affiliat (... [5])

Registrants may abuse the Add Grace Period for continual registration, deletion, and re-registration of the same names in order to avoid paying the registration fees. This practice is sometimes referred to as “domain kiting.” This term has been mistakenly used as being synonymous with *domain tasting*, but it refers to multiple and often consecutive tasting of the same domain name. ICANN staff has received anecdotal reports that this type of activity is occurring, but does not currently have data to demonstrate definitively that domain kiting occurs or to what extent.

The anecdotal reports received by the ICANN staff would indicate that:

- a. Very few registrants engage in kiting;
- b. Those registrars who facilitate kiting are discovered and warned by the registry to cease the behaviour;
- c. Kiting practices cannot enable a registrant to “keep” a single domain name. Any name is available to be taken in the drop pool by another registrant. The activity is only practicable if attempting to maintain a number of names – some would be lost at each drop.

5.9.2 Background

Bob Parsons appears to have introduced the term “domain kiting” in a blog post in 2006. In the post he chose to call the activity “kiting”, but his definition described what later came to be termed “domain tasting” (as The Public Interest Registry did in its letter to Steve Crocker on March 26, 2006). This confusion of terms carried forward for some time as can be seen in a MessageLabs report published several months later.

Eventually, the current definition of domain kiting (the serial re-registration of a domain to get a domain for free) solidified, but it is not clear whether it was based on any actual activity or whether it was simply a matter of repurposing an already confused definition to cover a possible abuse scenario. *Domain tasting* is a different practice, in which a registrant measures the monetization potential of a domain during the Add Grace Period, and deletes it in AGP if the domain is not worth keeping. In general, the goal of domain tasting is to retain registration of (and not delete) a “worthwhile” domain.

ICANN staff looked into domain kiting (while developing the 2007 I

Report on domain tasting) and could not find anything except anecdotal evidence of the activity. A RAPWG member performed an analysis of the .INFO registry in 2008 and again in December 2009, and did not find any examples of kiting. 1

5.9.3 Recommendations

1 <http://forum.icann.org/lists/gnso-rap-dt/msg00425.html>

- Refine the definitions of tasting and kiting based on the discussion and defined boundary conditions above.
- Incorporate these definitions in any review or refinement of excess-delete policy and data collection or data reporting efforts.
- Alert ICANN staff to the possibility of kiting as a possible abuse of the add-grace period.
- Check with other working groups (e.g. domain tasting) to determine if follow-on studies have useful definitions and data.
- Conduct broader research (at the registry level) to determine to what extent domain kiting is a problem.

| | | |
|---------------------------------|----------------|----------------|
| Page 73: [4] Change | - | 01/02/10 13:14 |
| Formatted Bullets and Numbering | | |
| Page 90: [5] Deleted | Marika Konings | 02/02/10 11:24 |

Annex III – Uniformity of Contracts: Additional Background Materials

Registry Agreement (RA) Dispersion:

Refer to the GNSO Issues Report on Registration Abuse Policies
Section 4 - Provisions in Registry Agreements relating to abuse
Pages 11 - 29

<http://gns0.icann.org/files/gns0/issues/registration-abuse/gns0-issues-report-registration-abuse-policies-29oct08.pdf>

Registry Registrar Agreement (RRA) Dispersion:

Refer to the GNSO Issues Report on Registration Abuse Policies
Section 4 - Provisions in Registry Agreements relating to abuse
Pages 11 - 29

<http://gns0.icann.org/files/gns0/issues/registration-abuse/gns0-issues-report-registration-abuse-policies-29oct08.pdf>

RRA Templates are contained within the RA and hence the analysis is combined with appendix 1.

Registrar Accreditation Agreement (RAA) Dispersion:

Because the RAA is template driven, a quick inventory of Registration Abuse Types (as defined by the RAPWG) was conducted within the RAA template instead of a formal dispersion study. Two RAAs exist. A version from May 2001 existed until the most recent May 2009 version was released. With over 80+% adoption rates by Registrars to the May 2009 version, it was the only RAA reviewed for dispersion.

<http://www.icann.org/en/registrars/agreements.html>

The May 2009 RAA does contain provisions that align with abuse types defined by the Working Group. These include WhoIS, UDRP, and Privacy language. However, the latest RAA does not contain any language relative to take-down, conduct & use, abuse definitions, and indemnification to protect parties from taking action against abuse.

In parallel to the RAPWG, a Working Group to enhance the RAA is underway. It is the UoC's intent to share any recommendations that appear to align with RAA WG actions. Based on the latest presentations from ICANN Seoul, WG members have already identified gaps around Malicious Conduct, Cybersquatting, Privacy/Proxy Services, and complete information disclosure with Affiliates & Resellers.

Registration Agreement (ra) Dispersion:

Refer to the GNSO Issues Report on Registration Abuse Policies
Section 5 - Provisions in Registration Agreements relating to abuse
Pages 30 - 37

<http://gnso.icann.org/files/gnso/issues/registration-abuse/gnso-issues-report-registration-abuse-policies-29oct08.pdf>

Registration Agreement (ra) Dispersion Study

An evaluation of publicly available online agreements (Domain Registration Agreement, Universal Terms of Service, etc.), from a representative sample of registrars was performed to determine the degree of variation among agreement provisions relative to abuse. This evaluation, essentially, is an inventory of sections within the registration agreement. It attempts to quantify "current state" for the purpose of providing a visual representation of dispersion.

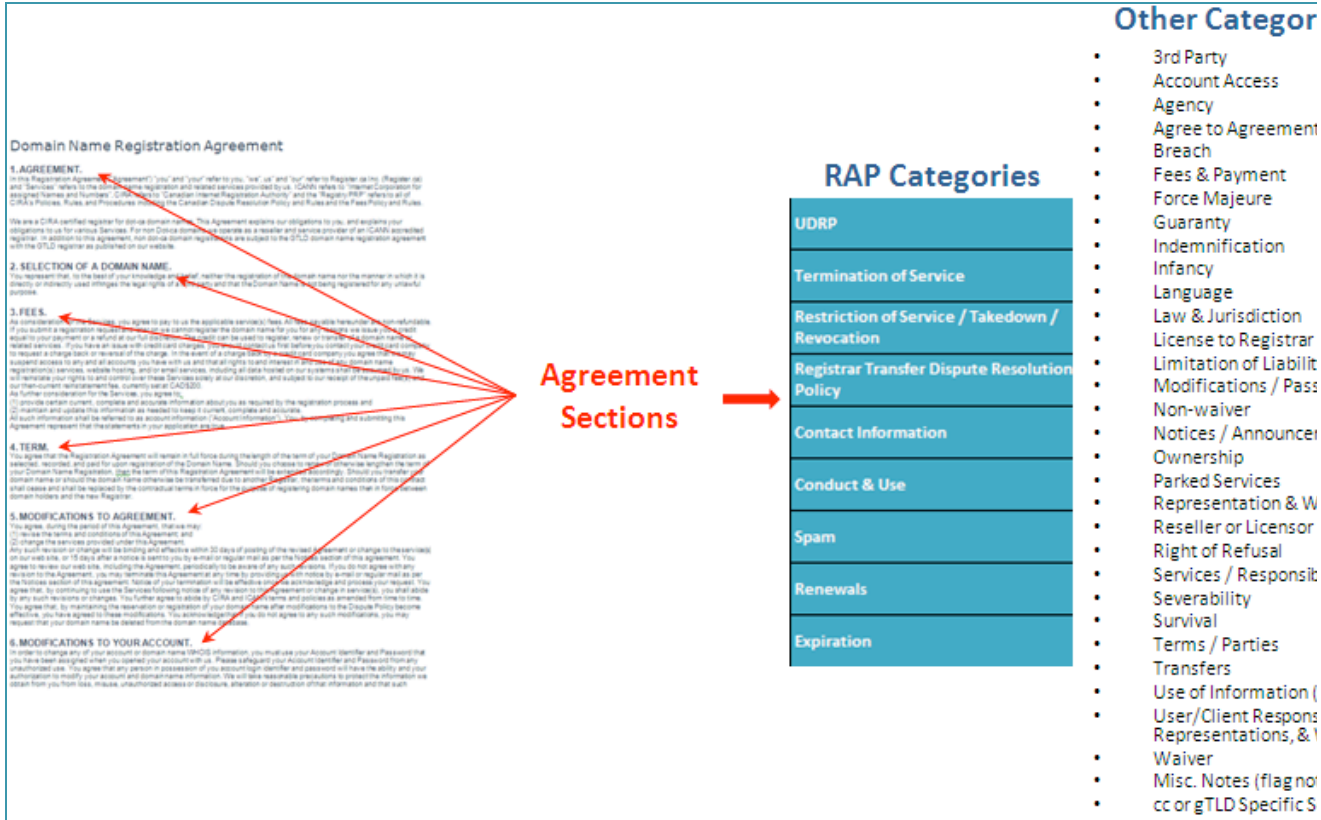
By review of the various registration agreements, sections began to naturally form in to forty or so categories in which the registration agreements could be inventoried. For each of the 22 Registrars, from the representative pool, an Excel spreadsheet was used to track the binary existence of each agreement category. If a category was found, the spreadsheet would be incremented accordingly, and if the section was relevant to abuse, the corresponding agreement language was pasted in to the spreadsheet. If no section was found, the category requirement was not met, nor was it incremented.

It should be noted, that this was not a compliance exercise, and as such, all results shared are anonymous. The representative sample of registrars is based on % market share of held registrations per webhosting.info as of June 2009. Within that sample, a general guiding principle for selection of the 22 registrars was the top, middle, and bottom market participants. This sample of 22 Registrars makes up approximately 59% of total market share. Additionally, the sample also attempts to gain representation across varying countries.

The actual spreadsheet and presentation reports can be found at the UoC Wiki Attachments section:

https://st.icann.org/reg-abuse-wg/index.cgi?uniformity_sub_team
RAPWG-UofC_Dispersion_Matrix_09152009.xls
RAPWG-UofC_Report_09152009.pdf

The diagram here shows a screen shot of a Registration Agreement (ra) on the left. Each red arrow points to a defined section within the agreement. On the right side of the diagram are the categories that formed from the inventory. Those labeled in the blue boxes pertain to the abuse types within scope of the RAPWG.

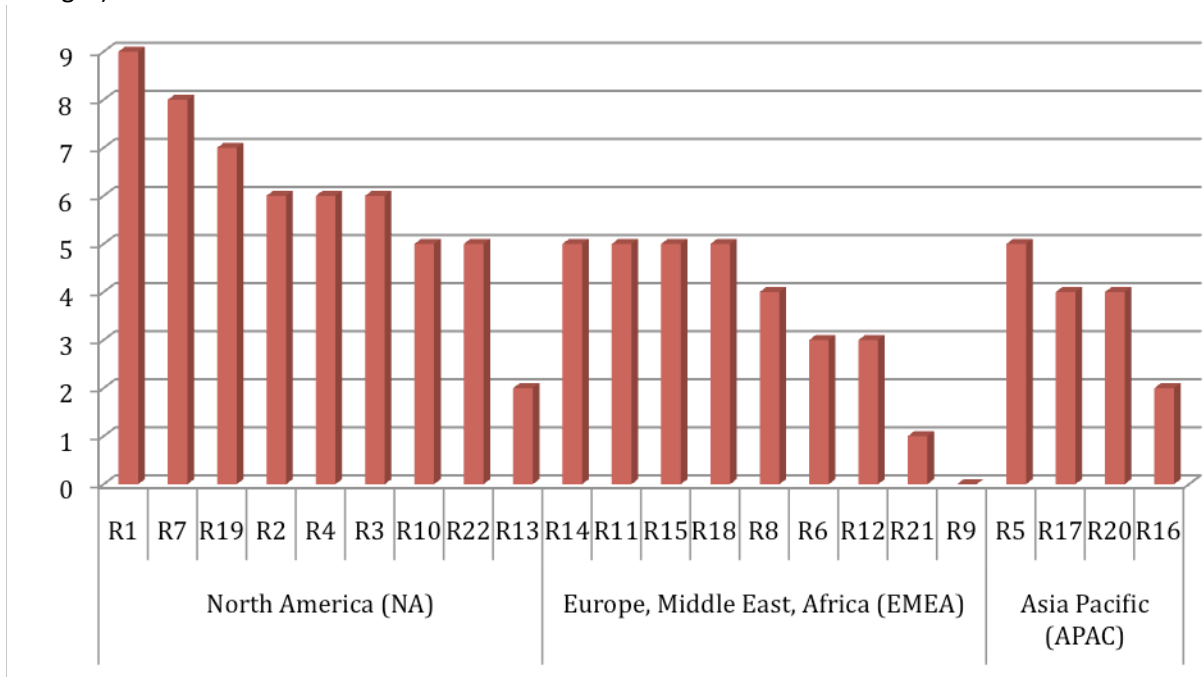


This screen shot represents the entire spreadsheet used to inventory Registration Agreement sections across the 22 Registrars. The zoom here is at 10%. This screen shot also includes those categories not relevant to abuse, and as such will not show pasted language from the agreement:

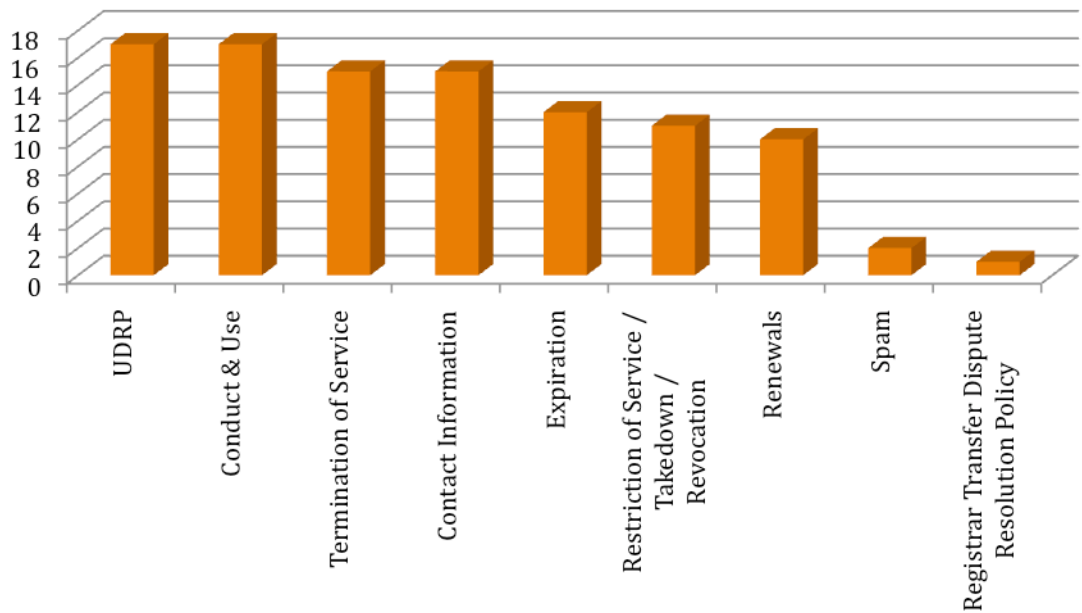
Legend:

| | |
|---|--|
| 1 | Agreement met category requirement by formal section definition |
| 0 | Category requirement flagged via separate agreement |
| 0 | Formal section definition of category not found within agreement |
| 0 | Tier 2 or 3 Agreement not found or not in scope |

The chart below provides a different view at the dispersion across Registration Agreements. The Y Axis represents the number of categories where the agreement satisfied the formal section definition requirements while the X Axis represents registrars by region, sorted highest to least (left to right).



This chart represents categories with the greatest achievement of section definition.



APB Example:

Definition of Abuse

a. Abuse is an action that: --- **(source: [RAP – WG Definition; DRAFT Only!](#))**-----

- i. Causes actual and substantial harm, or is a material predicate of such harm, and
- ii. Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed.

b. Domain abuse creates security and stability issues for the registry, registrars and registrants, as well as for users of the Internet in general. **<Registry>** defines abusive use as the wrong or excessive use of power, position or ability, and includes, without limitation, the following: ---

(source: [.info Domain Anti-Abuse Policy](#))-----

- i. Illegal or fraudulent actions;
- ii. Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service attacks;
- iii. Phishing: The use of counterfeit Web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data;
- iv. Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning;
- v. Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent.
- vi. Examples include, without limitation, computer viruses, worms, keyloggers, and Trojan horses;

vii. Fast flux hosting: Use of fast-flux techniques to disguise the location of Web sites or other Internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the Internet to which the domain name of an Internet host or name server resolves. Fast flux hosting may be used only with prior permission of Affiliates;

viii. Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks);

ix. Distribution of child pornography; and

x. Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

Indemnification - --- [\(source: .info Domain Anti-Abuse Policy & .org RRA - 3.6 Additional Requirements for Registration Agreement/3.65\)](#)-----

a. Pursuant to the RRA, <Registry> reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (3) to avoid any liability, civil or criminal, on the part of <Registry>, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement or (5) to correct mistakes made by <Registry> or any Registrar in connection with a domain name registration. <Registry> also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute. Abusive uses, as defined above, undertaken with respect to <TLD> domain names shall give rise to the right of <Registry> to take such actions under RRA in its sole discretion.