

## **Impact of Safeguards – New Version**

### **Background on Safeguards**

A key distinguishing feature of the New gTLD Program was the advent of additional safeguards aimed at protecting the integrity of the Domain Name System. The Government Advisory Committee (GAC) greatly influenced the development and adoption of many of the safeguards. In its Beijing Communiqué, the GAC advised that the safeguards proposed be subject to contractual oversight by ICANN and many have been implemented via contract provisions in the standard Registry and Registrar Agreements required for all new gTLDs.<sup>1</sup> However, a 2015 Review on the Effectiveness of GAC Advice observed that certain aspects of GAC advice were implemented differently from the way in which they were initially proposed.<sup>2</sup>

What follows is a discussion of certain key safeguards, focusing on the ability of the safeguard to be enforced via ICANN Contractual Compliance and/or to withstand challenges to potential enforcement.

### **Safeguards for all new gTLDs**

#### ***Whois verification***

The Whois verification requirements of the New gTLD Program sought to enhance abuse prevention and mitigation efforts.<sup>3</sup> The 2013 Registrar Agreement, which was mandatory for all new gTLD registrars, required adherence to the obligations specified in the Whois Accuracy Program Specification. Consequently, new gTLD registrars are required to engage in “reasonable and commercially practicable” Whois accuracy verification at the time of registration and periodic re-verification thereafter.<sup>4</sup>

Specifically, registrars are required to verify the syntax accuracy of registrant provided postal addresses, email addresses, and telephone numbers and verify the validity of the phone number and email address of the registrant. These provisions limit registrants to 7 days for correcting or updating such information and a total of 15 days for responding to inquiries by the

**Commented [1]:** This sentence is vague and inflammatory. The GAC did not provide implementation advice. The GAC provided policy advice and repeatedly insisted that it does not provide implementation advice. The GAC did assert that the NGPC did not accept an item of advice related to verification/validation. The Board later agreed with the GAC on this point. There has been no such agreement between the Board and the GAC however that “certain aspects of GAC advice were implemented differently from the way in which they were initially proposed.” This statement and the underlying issue are the subject of ongoing Board-GAC discussions. They have not reached conclusions like the one in this sentence.

<sup>1</sup> **Insert sites to standard Registry and Registrar contracts.**

<sup>2</sup> See GAC Advice Effectiveness Review, <https://gacweb.icann.org/display/gacweb/GAC+Correspondence> at January 29, 2016 at pp. 14-15 regarding review of Beijing Advice. The review noted that “the more the advice seeks to impose restrictions, safeguards, checks, rules, verification, authentication, other minimum behavioral expectations or ‘standard setting’, the less likely it is that ICANN will accept and implement the advice in the precise way that the GAC have requested.” P. 2.

<sup>3</sup> See “Mitigating Malicious Conduct,” ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

<sup>4</sup> Registrar Accreditation Agreement (June 2013), Section 3.7.8

registrar.<sup>5</sup> The consequences imposed by a registrar for a registrant's failure to comply include the suspension or cancellation of the domain name registration.<sup>6</sup>

ICANN contractual compliance reports indicate that WHOIS related complaints comprise the largest category of complaints that they receive related to registrars.<sup>7</sup> For example, of the 41,790 total complaints received in 2014, 29,857 related to WHOIS<sup>8</sup> (most complained about lack of accuracy) (about 71%). Of the 48,106 total complaints received in 2015, 36,354 related to WHOIS (again, accuracy) (about 75%).<sup>9</sup>

**Commented [2]:** Laureen's suggestion. See ICANN Contract Compliance Annual Reports [insert cites].

These figures indicate that the WHOIS safeguards created contract obligations that were sufficiently specific, that violations were flagged and generated complaints subject to the ICANN compliance process.<sup>10</sup>

Coinciding with the new WHOIS verification requirements and to improve the quality of contact data in the WHOIS, ICANN also implemented the WHOIS Accuracy Reporting System (ARS). The ARS is an effort to identify and report on accuracy in a systematic way. The GAC had advised Registry Operators be required to maintain statistical reports of inaccurate WHOIS records.<sup>11</sup> ARS is an ICANN project taken in part to respond to this GAC safeguard requiring documentation of WHOIS inaccuracies.<sup>12</sup> This implementation shifted the responsibility from Registry Operators to ICANN.<sup>13</sup> Originally, the ARS contemplated three phases: syntax accuracy; operability accuracy; and identity validation.<sup>14</sup>

To date, the ICANN ARS has only dealt with accuracy of syntax and operability (i.e., is the contact information in the correct format and is it an operating email, address or telephone number). The latest ARS Report was issued in June 2016 and contains findings on the accuracy of syntax (proper format) and operability (can it be used to communicate) of telephone numbers, postal address, and email address for a sample of both new and legacy gTLDs.<sup>15</sup> These

<sup>5</sup> Registrar Accreditation Agreement (June 2013) Section 3.7.7.1 and 3.7.7.2

<sup>6</sup> Registrar Accreditation Agreement (June 2013) Section 3.7.7.2

<sup>7</sup> See ICANN Contract Compliance Annual Reports [insert cites].

<sup>8</sup> Insert 2014 ICANN Annual Compliance report cites.

<sup>9</sup> Insert 2015 ICANN Annual Compliance report cites.

<sup>10</sup> See ICANN CCT Compliance Metrics 2014, 2015 at <https://www.icann.org/resources/reviews/cct/metrics>.

<sup>11</sup> [Beijing Communique: GAC Advice Effectiveness Review](#)

<sup>12</sup> The project aims to: proactively identify inaccurate gTLD registration data, explore the use of automated tools, forward potentially inaccurate records to registrars for action, and publicly report on the resulting actions to encourage improvement. See WHOIS Accuracy Reporting System <https://whois.icann.org/en/whoisars>

<sup>13</sup> [Beijing Communique; and GAC Advice Effectiveness Review; January 9, 2014](#) [insert cites]

<sup>14</sup> WHOIS Accuracy Reporting System at: <https://whois.icann.org/en/whoisars>

<sup>15</sup> See <https://whois.icann.org/en/whoisars-reporting>

findings indicate that new gTLDs have higher syntax accuracy ratings for email and telephone but lower syntax accuracy for postal address, when compared to legacy gTLDs.<sup>16</sup>

ICANN has not committed to progressing to the identity validation phase (i.e., is the individual listed responsible for the domain?).<sup>17</sup> Hence, the current documentation effort will only detect syntax and operability issues but will not detect and therefore not document inaccurate identity.<sup>18</sup>

Ultimately, specific language regarding WHOIS obligations and a detailed WHOIS specification may have promoted more focused efforts on combating abuse by creating clear obligations to gather specified information and hence promoting the ability to make actionable complaints to ICANN compliance.

Commented [3]: Source?

**Recommendations: 1.** ICANN should gather data to assess whether a significant percentage of WHOIS-related complaints relate to the accuracy of the identity of the registrant. This data should include analysis of WHOIS accuracy complaints received by ICANN compliance to identify the subject matter of the complaints (e.g. complaints about syntax, operability, or identity). ICANN should also identify other potential data sources of WHOIS complaints (registrars, registries, ISPs etc.) and attempt to obtain anonymized data from these sources.

**2.** If identity is a significant percentage of complaints, then the ICANN Board should direct ICANN to proceed with the identity phase of ARS project.

**Rationale/Related findings:** WHOIS-related complaints are the largest category of complaints received by ICANN Compliance for Registrars. However, it is unclear what aspect of WHOIS accuracy forms the basis of these complaints. Although Phase 1 of ICANN's ARS project analyzes the syntax accuracy of WHOIS contact information and Phase 2 assesses the operability of the contact data in the WHOIS record, there is currently no plan to proceed with Phase 3 of the ARS project, identity validation (is the contacted individual responsible for the domain?).

**To:** ICANN Board and ICANN staff.

**Must be completed prior to subsequent rounds:** No.

**Consensus within team:** Yes

<sup>16</sup> See Phase 2 ARS Report at [https://whois.icann.org/en/file/whois-ars-phase-2-cycle-2-report-syntax-and-operability-accuracy \(applying 2013 RAA criteria for syntax\)](https://whois.icann.org/en/file/whois-ars-phase-2-cycle-2-report-syntax-and-operability-accuracy%20(applying%202013%20RAA%20criteria%20for%20syntax))

<sup>17</sup> WHOIS Accuracy Reporting System <https://whois.icann.org/en/whoisars>

<sup>18</sup> WHOIS Accuracy Reporting System <https://whois.icann.org/en/whoisars>

### **Mitigating abusive activity**

The Base Registry Agreement required new gTLD registry operators to include provisions in their Registry-Registrar agreements that prohibited registrants from “distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.”<sup>19</sup> By its terms, this safeguard is aimed at mitigating abusive activity. This provision was incorporated into the mandatory public interest commitments (PICs) section of the Registry agreement.

Notably, the plain language of the safeguard does not obligate the Registry operator to monitor and enforce this provision beyond requiring the inclusion of the provision in the downstream Registrar-Registrant agreement. ICANN concluded that 99% of new gTLD registry operators had complied with the obligation to include this language in their Registry-Registrar agreements by the end of 2014.<sup>20</sup>

Complementing the prohibited use provisions, new gTLD registrars were bound by the 2013 RAA, which imposed on registrars a duty to promptly “investigate and respond appropriately to any reports of abuse.”<sup>21</sup> Subsequently, ICANN received abuse complaints in 2014, 2015, and 2016.<sup>22</sup> Abuse complaints are typically higher for registrars than registries. In 2015, ICANN received 438 abuse complaints related to Registrars.<sup>23</sup> These complaints included both legacy and new gTLDs. ICANN noted that these complaints involved in part, “Registrars not taking reasonable and prompt steps to respond to appropriately to reports of abuse, which at a minimum should be to forward valid complaints to the registrants.”<sup>24</sup> ICANN’s 2015 audit of registrars under the 2013 RAA indicated that 74% of the registrars audited had deficiencies related to the RAA contract provisions requiring a Registrar Abuse Contact and a duty to investigate complaints of abuse.<sup>25</sup> ICANN’s 2016 audit of registrars showed a deficiency rate of 60% related to this same contract provision.<sup>26</sup> These figures indicate that the Mitigating Abuse Safeguard is the subject of complaints and the ICANN compliance process.<sup>27</sup>

**Commented [4]:** Carlton’s comment: I think it is our duty to say that figures from reputable third party sources record much higher numbers of abuse! **LK:** Carlton, please suggest sources that support this statement. We can add in a fn.

<sup>19</sup> Base Registry Agreement (updated 1/9/2014) Specification 11, 3(a).

<sup>20</sup> See 2014 ICANN Contract Compliance Annual Report at p 13.

<sup>21</sup> RAA 3.18, <https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en>

<sup>22</sup> See Contractual Compliance Annual Reports for 2014 and 2015 and quarterly reports for 2016.

<sup>23</sup> 2015 ICANN Contractual Compliance Annual Report.

<sup>24</sup> 2015 ICANN Contractual Compliance Annual Report.

<sup>25</sup> ICANN Contractual Compliance September 2015 Round Audit Report at <https://www.icann.org/en/system/files/files/compliance-registrar-audit-report-2015-06jul16-en.pdf>

<sup>26</sup> ICANN Contractual Compliance May 2016 Round Audit Report at <https://www.icann.org/en/system/files/files/compliance-registrar-audit-report-2016-16nov16-en.pdf>

<sup>27</sup> The effectiveness of this safeguard and ICANN Compliance’s enforcement of this safeguard has been the topic of Congressional Testimony. See e.g., <https://www.judiciary.senate.gov/imo/media/doc/09-14-16%20Horton%20Testimony.pdf> (arguing that ICANN Compliance efforts regarding registrars that allegedly failed

It is not clear whether these safeguards have had an impact on mitigating abuse. It is also not clear what constitutes “reasonable and prompt steps to respond to appropriately to reports of abuse.”

**Recommendation:** Continue to gather data comparing rates of abuse in domains operating under new Registry Agreement and Registrar Agreements to legacy gTLDs.

**Commented [5]:** Margie's comment: are these before the next round? What is the goal of the data requests or surveys? is it a one time or ongoing requirement

**Rationale/Related findings:** In order to better measure new gTLDs’ ability to mitigate abusive activity, data related to abuse rates in new gTLDs should be gathered and analyzed on a regular basis. The data should be reviewed by both the ICANN organization and be made available to future review teams. The CCT Review team has commissioned a study on this topic to serve as a baseline for future review teams and will report findings based on this study in our Final Report.

**To:** ICANN organization

**Must be completed prior to subsequent rounds:** No

**Consensus within team:** Yes

### **Security checks**

Another mandatory PIC that is included in the new gTLD Registry Agreement required that registry operators “periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets.”<sup>28</sup> Furthermore, this safeguard obligated registry operators to maintain statistical reports on such threats and mitigation efforts, making them available to ICANN upon request.<sup>29</sup> This safeguard was intended to enhance efforts to fight DNS abuse.<sup>30</sup>

GAC advice had also included an enforcement mechanism that called for a Registry Operator to notify a Registrar if the detected threats pose an actual risk of harm and provides for suspension of a domain name until a matter is resolved if the Registrar fails to act.<sup>31</sup> However, ICANN reported community concerns about the timing, cost, and scope of conducting security checks for threats.<sup>32</sup> Hence, the safeguard implementation provided “general guidelines for what registry operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security

---

to investigate and respond to complaints that domain names were being used to facilitate illegal activity were ineffective and lacked transparency).

<sup>28</sup> Base Registry Agreement (updated 1/9/2014) Specification 11, 3(b).

<sup>29</sup> Base Registry Agreement (updated 1/9/2014) Specification 11, 3(b).

<sup>30</sup> <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

<sup>31</sup> Beijing Communiqué.

<sup>32</sup> See <https://features.icann.org/safeguards-applicable-all-new-gtlds>

checks.”<sup>33</sup> Nevertheless, as implemented by ICANN, the safeguard lacks obligations on either notification to the Registrar or how to respond to security threats.

The obligation to engage in security checks can be enforced, as implemented.<sup>34</sup> ICANN compliance reports engaging in proactive monitoring of this safeguard and determined for example, that 96% of registries were conducting security checks as per the contract.<sup>35</sup> Community discussions on how to develop a framework for registry operators to conduct periodic security checks and respond to identified security threats are currently underway.<sup>36</sup>

**Recommendation:** review the proposed Registry Operator Framework when completed and assess whether the framework is a sufficiently clear and effective mechanism to mitigate abuse by providing for specified actions in response to security threats.

**Rationale/Related findings:** It is not clear whether the intended goal of the security checks safeguard – to enhance efforts to fight DNS abuse – has been met. The community will be better positioned to evaluate the effectiveness of this safeguard once a specific framework has been proposed that specifies how Registry Operators should respond to Security Threats.

**To:** Community Stakeholders and future review teams.

**Must be Completed Prior to Subsequent Rounds:** No.

**Consensus within Team:** Yes.

### ***Making and Handling Complaints***

The Base Registry Agreement for new gTLDs required registry operators to “take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD” with the caveat that they would “not be required to take any action in contravention of applicable law.”<sup>37</sup> Furthermore, new gTLD registry operators were obligated to

---

<sup>33</sup> <https://features.icann.org/safeguards-applicable-all-new-gtlds>

<sup>34</sup> The GAC Advice Effectiveness Review questioned the effectiveness of this safeguard noting that “risks may be identified but not necessarily acted on.” GAC Advice Effectiveness Review, at <https://gacweb.icann.org/display/gacweb/GAC+Correspondence> at January 29, 2016 at pp. 12-13.

<sup>35</sup> ICANN 2014 Contractual Compliance Report at p. 13 (2014 Registry Compliance Summary).

<sup>36</sup> <https://myicann.org/plan/project/54398430005f4feb0a04e53e8afaa73b>

<sup>37</sup> Base Registry Agreement (updated 1/9/2014), Section 2.8, Protection of Legal Rights of Third Parties

post abuse contact details on their websites and notify ICANN of any changes to contact information.<sup>38</sup>

These safeguards, like others, were aimed at enabling more focused mitigation of DNS abuse<sup>39</sup> and created a duty for registry operators to investigate and respond to complaints from government agencies but not the public. GAC advice did not propose such a restriction.<sup>40</sup>

Data from Nielsen's Consumer surveys indicate that many consumers remain unaware of to whom to report abuse. Specifically, 31% overall "don't know" who to report site abuse to, 31% overall would report abuse to a consumer protection agency, 30% overall would report abuse to local police, 24% overall would report abuse to website owner or operator, and 11% overall would report abuse to ICANN.<sup>41</sup>

The GAC questioned the specifics of implementation, specifically asking "what constitutes reasonable steps" to investigate and respond to complaints and noting that the effectiveness of this safeguard depends on whether Registry Operators "have a responsibility to respond to complaints from sources other than governments or law enforcement agencies."<sup>42</sup> ICANN's 2014 Contractual Compliance report noted that Registry Operators "not publishing the email address and primary contact for reports by mail" and "Registry Operators not responding in a timely matter" were a common contractual compliance issue regarding publishing abuse contact information.<sup>43</sup> Hence, this safeguard can be the subject of complaints and the ICANN compliance process.

The obligation to have mechanisms to respond to complaints likely assists Registries to investigate and possibly combat abuse and may help protect the public by providing information about harmful practices. However, questions remain about the scope of Registry Operators' response under this safeguard both as to its duty to investigate and respond to complaints from law enforcement and its responsibility to respond to complaints from the public.

**Recommendations:** 1. Assess whether mechanisms to report and handle complaints has led to more focused efforts to combat abuse by determining a) the volume of reports of illegal

---

<sup>38</sup> Base Registry Agreement (updated 1/9/2014), Specification 6, Section 4,1, Abuse Mitigation.

<sup>39</sup> See "Mitigating Malicious Conduct," ICANN, New gTLD Program Explanatory Memorandum, 3 October 2009, <https://archive.icann.org/en/topics/new-gtlds/mitigating-malicious-conduct-04oct09-en.pdf>

<sup>40</sup> [Beijing Communique \[insert cite\]](#) See also 2014 Singapore Communique (questioning what mechanisms could be used by *victims* (in addition to law enforcement) to report abuse to Registry Operators and what constitutes "reasonable steps" to investigate and respond to reports from law enforcement or other governmental bodies.

<sup>41</sup> Nielsen June 2016 Survey at pp.88, 102

<sup>42</sup> See e.g., Singapore 2014 Communique at p. 10 (Attachment regarding Safeguard 5); GAC Advice Effectiveness Review, <https://gacweb.icann.org/display/gacweb/GAC+Correspondence> at January 29, 2016 at p.13..

<sup>43</sup> (at p. 14).

conduct in connection with the use of the TLD that Registries receive from government and quasi-governmental agencies and the volume of inquires that Registries receive from the public related to malicious conduct in the TLD and b) what actions Registries take to respond to complaints of illegal or malicious conduct in connection with the use of the TLD. Such an effort could include surveys, focus groups, or community discussions.

2. Assess whether more efforts are needed to publicize where the complaints that involve abuse or illegal behavior within a TLD should be directed.

**Rationale/Related findings:** Although implementation of the safeguards regarding making and handling complaints have been implemented, it is unclear: 1) whether either law enforcement or the public are sufficiently aware that these complaint mechanisms exist; 2) how frequently these channels are used by the public and law enforcement to notify registries of illegal or abusive behavior; and 3) what impact these safeguards have had on their intended goal of mitigating DNS abuse.

**To:** ICANN Board

**Must be Completed Prior to Subsequent Rounds:** No.

**Consensus within Team:** Yes.

#### **Safeguards for sensitive and regulated strings**

The GAC identified a non-exhaustive group of nearly 200 strings (Category 1) that raised consumer protection concerns, contained sensitive strings, or strings in regulated markets and advised that five safeguards should apply to these Category 1 strings. The GAC explained that strings linked to “regulated or professional sectors should operate in a way that is consistent with applicable laws” and observed that the identified strings were “likely to invoke a level of implied trust from consumers, and carrier higher levels of risk associated with consumer harm.”<sup>44</sup> During implementation, however, ICANN included only a subset of these GAC-identified strings within the Category 1 safeguard protections.<sup>45</sup> In addition, during

---

<sup>44</sup> GAC Beijing Communique, Annex 1, Safeguards on New gTLDs at p. 8.

<sup>45</sup> Compare Beijing Communique to ICANN Implementation Framework for GAC Category 1 Implementation Advice, see <https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards>; and <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>, October 29, 2013 letter Crocker to GAC Chair; September 2, 2014 letter Crocker to GAC Chair; and June 23, 2015 Crocker to GAC Chair.



implementation, ICANN included only three of the five GAC-recommended safeguards to its selected subset of Category 1 strings in regulated markets.<sup>46</sup>

As implemented, these safeguards took the form of downstream contract requirements contained in the Public Interest Commitments Specification of the Registry Agreement. Specifically, the safeguards required registry operators to obligate registrars vis-à-vis the Registry-Registrar Agreement to include certain provisions in their Registration Agreements with Registrants.

The requirements for sensitive strings and those in regulated markets included provisions requiring registrants to comply with all applicable laws.<sup>47</sup> Another provision emphasized that this obligation includes “those [laws] that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.”<sup>48</sup> Furthermore, specific provisions detailed requirements for registrants handling sensitive information, such as health or financial data, to “implement reasonable and appropriate security measures commensurate with the offering of those services, as defined by applicable law.”<sup>49</sup>

**Commented [6]:** Could not find this quote in the link provided. Need to check that links in this section are correct. LK: See fn. This is in Annex 2 of the Board's Resolution re: new gTLDs dated 2/5/14.

It is difficult to determine whether these safeguards have been the subject of complaints to ICANN contract compliance because the categories of complaints identified in ICANN's Compliance Reports do not provide this level of detail. That is, the reported ICANN complaint categories for Registries and Registrars such as “PIC” (Public Interest Commitments) or “Abuse,” do not contain sufficiently specific information to correlate complaints with specific safeguards. ICANN Compliance does report that it proactively monitored compliance with Specification 11, ¶13a that includes the obligation for downstream contracts to include language requiring compliance with applicable laws, and determined that there was 99% compliance with this provision.<sup>50</sup>

**Recommendations:** 1. Include more detailed information on subject matter of complaints in ICANN publicly available Compliance Reports. Specifically, more precise data on the subject

<sup>46</sup> Compare Beijing Communique to ICANN Implementation Framework for GAC Category 1 Implementation Advice, see <https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards>; and <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>. See also October 29, 2013 letter Crocker to GAC Chair; September 2, 2014 letter Crocker to GAC Chair.

<sup>47</sup> January 9, 2014 Registry Agreement (standard Registry Agreement), Specification 11, 3(f)

<sup>48</sup> ICANN Implementation Framework for GAC Category 1 Implementation Advice, see <https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards>; and <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

<sup>49</sup> ICANN Implementation Framework for GAC Category 1 Implementation Advice, see <https://newgtlds.icann.org/en/applicants/gac-advice/cat1-safeguards>; and <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

<sup>50</sup> ICANN 2014 Contractual Compliance Report at p.13.

matter of complaints, particularly 1) what type of law violation is being complained of and 2) an indication of whether complaints relate to the protection of sensitive health or financial information, would assist future review teams in their assessment of these safeguards. **Note:** A general recommendation for further transparency regarding the subject matter of complaints received by ICANN Compliance is set forth in **[insert site to Data Analysis paper and Recommendation]**

2. Initiate discussions with relevant stakeholders to determine what constitutes reasonable and appropriate security measures commensurate with the offering of services that involve the gathering of sensitive health and financial information. Such a discussion could include identifying what falls within the categories of “sensitive health and financial information” and what metrics could be used to measure compliance with this safeguard.

**Rationale/Related findings:** The lack of publicly available information about whether ICANN Compliance has received complaints related to the implemented Category 1 safeguards, and lack of a common framework to define sensitive information and identify what constitutes “reasonable and appropriate security measures” makes it difficult to assess what impact this safeguard has had on mitigating risks to the public.

**To:** ICANN Board

**Must be Completed Prior to Subsequent Rounds:** No.

**Consensus within Team:** Yes.

### **Safeguards for highly-regulated strings**

The GAC advised that strings associated with market sectors that have clear and/or regulated entry requirements in multiple jurisdictions (such as: financial, gambling, professional services, environmental, health and fitness, corporate identifiers, and charity) should also receive protections in the form of three additional safeguards.<sup>51</sup> The GAC explained that these strings may require additional safeguards to address specific risks and to “bring registry policies in line with arrangements in place offline.”<sup>52</sup> As implemented by ICANN, the safeguards applied to about 50 strings but received fewer protections than GAC had originally advised.<sup>53</sup>

---

<sup>51</sup> See Beijing Communique at Annex 1 pp. 8-10 (Category 1 Safeguards).

<sup>52</sup> Beijing Communique at Annex 1 p. 10.

<sup>53</sup> Compare Beijing Communique to <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>. See also GAC Advice Effectiveness Review at Appendix One regarding Beijing Advice (Category 1 Consumer Safeguards at pp. 14-15 and June 23, 2015 letter Crocker to GAC Chair.

As with the other safeguards, many of these safeguards imposed downstream contract requirements upon registry operators to obligate registrars vis-à-vis the Registry-Registrar Agreement to include certain provisions in their Registration Agreements with Registrants. The five additional safeguards that applied to strings in highly-regulated markets related to relationships with regulatory and industry bodies, providing contact information to report complaints, and screening for proper credentials for strings in highly- regulated markets.

Specifically, Registry operators were obligated to establish relationships with the relevant regulatory and industry bodies to mitigate risks of illegal activity.<sup>54</sup> Moreover, the standard contracts needed to include provisions that would require registrants to have a single point of contact for complaint reporting and contact information for relevant regulatory bodies.<sup>55</sup> Regarding the requirement to establish relationships with relevant regulatory/industry bodies, implementation of this provision appears to be satisfied by the mere issuing of an invitation to have a relationship.<sup>56</sup> This implementation may reflect the practical challenges involved with mandating a relationship with a third-party organization. In terms of effectiveness, more information is needed on Registry efforts to comply with this safeguard. Regarding the requirement for registrants to provide contact information for complaints and information about relevant regulatory bodies, a key question would be how easy it is for the public to find information on a website regarding contact information for communicating complaints both to those responsible for the domain and applicable government agencies or regulatory bodies.

The final three safeguards related to the credentialing that registrants possessed relating to strings in highly- regulated markets. The GAC had recommended that Registry Operators 1) verify and validate registrants' credentials "at the time of registration", 2) consult with authorities in case of doubt, and 3) conduct periodic post-registration checks to ensure registrants' validity.<sup>57</sup> As implemented by ICANN, Registry Operators were only required to ensure that registrars included in their agreement with registrants a provision requiring a representation that the "registrant possesses any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD."<sup>58</sup> Registry operators were obligated to investigate the authenticity of a registrant's credentials only if they received a complaint casting doubt on them.<sup>59</sup> Finally, registrars, vis-à-vis the

---

<sup>54</sup> <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>.

<sup>55</sup> <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>.

<sup>56</sup> [Base Registry Agreement for highly regulated strings. "Registry operators will proactively create a clear pathway for the creation of a working relationship with the relevant regulatory or industry self-regulatory bodies by publicizing a point of contact and inviting such bodies to establish a channel of communication..."](#)

<sup>57</sup> ICANN Implementation Framework for GAC Category 1 Implementation Advice at ¶¶ 6-8, <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

<sup>58</sup> ICANN Implementation Framework for GAC Category 1 Implementation Advice at ¶6 <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

<sup>59</sup> ICANN Implementation Framework for GAC Category 1 Implementation Advice at ¶7, <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

Registry-Registrar Agreement, were obligated to require their registrants to report “any material changes to the validity” of their credentials.<sup>60</sup>

These provisions were designed to mitigate the higher levels of risks of abuse associated with strings in highly-regulated industries, which are likely to invoke a higher level of trust to consumers.<sup>61</sup> The Nielsen Consumer End-User and Registrant Surveys indicated that consumers expect restrictions on who can purchase new gTLDs and that restrictions on who can purchase new gTLDs contribute to consumer trust.<sup>62</sup> GAC advice originally tasked registries with screening registrants for proper credentials or licenses at the time of registration to ensure that they are what they purport to be before they may do business with the public using the name of a regulated sector such as a bank or pharmacy. As implemented by ICANN, registrants themselves were to self-report that they possessed the necessary credentials. The GAC indicated that the looser requirement that registrants provide some “representation” that they possess the appropriate credentials (e.g. as a bank, insurer, pharmacy, etc.) poses the risk of consumer fraud and potential harm because bad actors will not hesitate to make false representations about their credentials.<sup>63</sup>

The ICANN Board indicated that its implementation approach resulted from concerns about the practical ability to implement these safeguards as advised because of challenges involved in verifying credentials of entities in multiple jurisdictions.<sup>64</sup>

#### Recommendations:

- 1) Survey a sample of Registries to determine what steps they are taking to establish working relationships with relevant government or industry **bodies**.
- 2) Survey a sample of Registrants to determine the volume of complaints they are receiving from regulatory bodies and their standard practices to respond to those complaints.
- 3) Assess a sample of domain websites within the highly-regulated sector category to see whether contact information to file complaints is sufficiently easy to find.
- 4) Assess whether restrictions regarding possessing necessary credentials are being enforced by auditing registrars and resellers offering the highly-regulated TLDs (i.e., can an individual or entity without the proper credentials buy a highly regulated domain?).

**Commented [7]:** Carlton's comment: See comment above. Do we want a survey or should we recommend these be indicators for ICANN compliance reportage and should be institutionalized?

<sup>60</sup> ICANN Implementation Framework for GAC Category 1 Implementation Advice at ¶18, <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

<sup>61</sup> See Beijing and London Communiqués.

<sup>62</sup> [Nielsen, Phase 1, ICANN Global Consumer Research Study p.9-10, 25-26, 44; Nielsen, Phase 2, ICANN Global Consumer Research Study p.9, 13, 26, 60](#) ; [Nielsen, Wave 2, ICANN Global Registrant Survey p. 14, 18, 29, 67.](#)

<sup>63</sup> See e.g., GAC 2014 London Communiqué at p. 10. See also, GAC 2014 Singapore Communiqué at p.4 and p. 10; and 2014 Los Angeles Communiqué at p.5 (all questioning ICANN's failure to implement the GAC's advice regarding verification and validation of credentials for strings in highly regulated markets).

<sup>64</sup> See e.g. Board Chair correspondence to GAC Chair , October 29, 2013 and; Sept. 2, 2014.

- 5) Determine the volume and subject matter of complaints regarding domains in highly-regulated industries by seeking more detailed information from ICANN compliance and registrar/resellers of highly regulated domains.
- 6) Compare rates of abuse between those highly-regulated gTLDs who have voluntarily agreed to verify and validate credentials to those highly-regulated gTLDs that have not.

**Rationale/Related findings:** Although ICANN has implemented certain safeguards applicable to domains for highly regulated strings, it is unclear whether and how contracted parties are complying with these safeguards. It is also not clear whether these safeguards have been effective in mitigating risks associated with domains in highly-regulated markets.

**To:** ICANN Board

**Must be Completed Prior to Subsequent Rounds:** Yes.

**Consensus within Team:** Yes.

#### **Special Safeguards related to new gTLDs with inherent governmental functions and Cyberbullying**

The Base Registry Agreement included provisions for operators of new gTLDs with inherent governmental functions, such as .army, .navy, and .airforce, to mandate that their registrars to ensure that their registrants “take reasonable steps to avoid misrepresenting or falsely implying” that the registrant was associated with a governmental authority when such a relationship did not exist.<sup>65</sup>

Another safeguard was related to cyberbullying and harassment and applied to the .fail, .gripe, .sucks, and .wtf gTLDs. This provision required registry operators to “develop and publish registration policies to minimize the risk of cyber bullying and/or harassment.”<sup>66</sup>

It is not clear whether failure to comply with these safeguards has generated complaints. In addition, as advised and implemented, neither safeguard contains consequences for failure to comply, raising questions about their effectiveness.

---

<sup>65</sup> <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

<sup>66</sup> <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-2-05feb14-en.pdf>

**Recommendations:** 1. Determine whether ICANN Compliance has received complaints for a Registry Operator's failure to comply with either the safeguard related to gTLDs with inherent governmental functions or the safeguard related to cyberbullying.  
2. Survey Registries to determine how they enforce these safeguards.

**Rationale/Related findings:** The lack of information about whether ICANN Compliance or Registries have received complaints related to these safeguards and lack of consequences for failure to comply with these safeguards makes it difficult to assess their effectiveness in mitigating the risks they were intended to address,

**To:** ICANN Board.

**Must be Completed Prior to Subsequent Rounds:** No.

**Consensus within Team:** Yes.

### **Restricted Registration Policies**

ICANN implemented safeguards applicable to restricted registration policies noting that restricted access was "an exception to the general rule that the gTLD domain name space is operated in an open manner."<sup>67</sup> These safeguards arose from GAC's Category 2 safeguard advice. ICANN implemented these recommendations by incorporating provisions into the Base Registry Agreement to 1) mandate that registries operate in "a transparent manner consistent with general principles of openness and non-discrimination by establishing, publishing and adhering to clear registration policies."<sup>68</sup> and 2) prevent "Generic String" registry operators from restricting registration eligibility to a "single person or entity and/or that person's or entity's 'Affiliates'".<sup>69</sup> The GAC had originally advised to ensure that registration restrictions were appropriate for risks associated with particular gTLDs.<sup>70</sup> Subsequent GAC advice reflects

---

<sup>67</sup> Beijing Communique at Annex 1 pp. 10-11 (Category 2 Safeguards).

<sup>68</sup> ICANN NGPC Resolution 2013.06.25.NG04 - 2013.06.25.NG05 - 2013.06.205.NG06  
<https://features.icann.org/category-2-safeguard-advice-re-restricted-and-exclusive-registry-access> and <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-i-agenda-2c-25jun13-en.pdf>

<sup>69</sup> ICANN NGPC Resolution 2013.06.25.NG04 - 2013.06.25.NG05 - 2013.06.205.NG06  
<https://features.icann.org/category-2-safeguard-advice-re-restricted-and-exclusive-registry-access> and <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-i-agenda-2c-25jun13-en.pdf>

<sup>70</sup> Beijing Communique at Annex 1 pp. 10-11 (Category 2 Safeguards).

ongoing concerns about whether restricted registration policies could lead to undue preferences.<sup>71</sup>

The ICANN Global surveys indicated that the public expects certain restrictions about who can purchase domain names and trusts that these restrictions will be enforced.<sup>72</sup> The survey results also indicated that the presence of such restrictions contributed to consumer trust.<sup>73</sup> An upcoming study on DNS Abuse may provide information that correlates the presence or absence of registration restrictions with rates of DNS abuse.

Commented [KL8]:

**Recommendations:** 1. Collect data comparing trustworthiness of new gTLDs with restrictions on registration to new gTLDs with few or no restrictions.

2. Repeat/refine DNS Abuse Study to determine whether presence of additional registration restrictions correlates to decrease in abuse.

Commented [9]: Delete "upcoming"

Commented [10]: Margie's edit

3. Collect data weighing cost/benefits of implementing various registration restrictions, including impact on compliance costs and costs for Registries, Registrars, and Registrants. One source of this data might be existing gTLDs for information (for example for verification/validation restrictions, could look to those new gTLDs that have voluntarily included verification/validation requirements to get a sense of costs involved).

4. Gather public comments on the impact of new gTLD registration restrictions on competition to include whether restrictions have created undue preferences.

**Rationale/Related findings:** The Nielsen surveys indicated a positive relationship between registration restrictions and trustworthiness of a domain. However, in addition to benefits, registration restrictions may also impact competition. More information is needed to assess

---

<sup>71</sup> See e.g., 2013 Buenos Aires Communique; 2014 Singapore Communique; 2014 Los Angeles Communique; 2014 London Communique ( Regarding implementation of the GAC Category 2 safeguard advice: "The NGPC should reconsider its position, particularly since the GAC has clearly advised that it does not believe the current requirements in Specification 11 actually meet either the spirit or the intent of the GAC's advice")

<sup>72</sup> Wave 2, ICANN Global Consumer Research Study p.9, 13, 26-27, 65; Nielsen, Wave 2, ICANN Global Registrant Survey p. 14, 18, 30, 68.

<sup>73</sup> Wave 1, ICANN Global Consumer Research Study p.9, 26; Nielsen, Wave 2, ICANN Global Consumer Research Study p.9, 13, 26,

whether this safeguard has met its intended goal in a manner that balances the benefits to the public in terms of trustworthiness and competition.

**To:** ICANN Board, PDP Working Group, and future CCT review teams.

**Must be Completed Prior to Subsequent Rounds:** Yes.

**Consensus within Team:** Yes.