

**ANNEX 1 to NGPC Resolution 2014.06.06.2c**  
**GAC Advice (Singapore, Buenos Aires, Durban, Beijing): Actions and Updates**  
**(As of 2 June 2014)**

Text Superseded by Scorecard Adopted as Annex 1 to NGPC Resolution 2014.06.06.NG02: <https://www.icann.org/en/system/files/files/resolutions-new-gtld-annex-1-06jun14-en.pdf>





**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

	Question	Response
<b>0. GAC Advice Implementation Questions for Singapore, March 2014</b>		
1.	<p>Will ICANN provide periodic updates to the GAC regarding the activities carried out by the Compliance Department on the effective implementation of the Safeguards (all categories)?</p>	<p>ICANN stands ready to provide periodic updates to the GAC regarding the activities carried out by the Compliance Department on the effective implementation of the Safeguards, including possibly at ICANN meetings, or through webinars. ICANN looks forward to hearing from the GAC about establishing convenient times and methods of providing the updates that would be informative and effective for GAC members.</p> <p>In the meantime, please refer to the different links below for published material about ICANN Contractual Compliance activities and updates.</p> <ol style="list-style-type: none"> <li>1. For monthly briefings on compliance activities, refer to <a href="http://www.icann.org/en/resources/compliance/update">http://www.icann.org/en/resources/compliance/update</a></li> <li>2. For monthly statistical reporting across the regions, the compliance types and reporters, refer to <a href="https://features.icann.org/compliance">https://features.icann.org/compliance</a></li> <li>3. To learn more about the most common complaints ICANN receives that may be in violation of the agreements and/or consensus policies, refer to <a href="http://www.icann.org/en/resources/compliance/complaints">http://www.icann.org/en/resources/compliance/complaints</a></li> <li>4. For the latest Notices of Breach, Suspension, Termination and Non-Renewal, refer to <a href="http://www.icann.org/en/resources/compliance/notices">http://www.icann.org/en/resources/compliance/notices</a></li> <li>5. For the ICANN Contractual Compliance Annual Report, refer to <a href="http://www.icann.org/en/resources/compliance/reports">http://www.icann.org/en/resources/compliance/reports</a></li> <li>6. For the Audit Program, refer to <a href="http://www.icann.org/en/resources/compliance/audits">http://www.icann.org/en/resources/compliance/audits</a></li> </ol>

**1. Safeguards Applicable to all New gTLDs**

With regard to **Safeguard 1**, related to WHOIS verification and checks, the NGPC has shifted responsibility from individual Registry Operators (who have the direct relationships with Registrars) to ICANN to perform “periodic sampling” of WHOIS data across registries in an effort to identify potentially inaccurate records.

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

1.	Can the NGPC clarify the advantages and/or disadvantages of having ICANN perform the WHOIS checks/audits versus the Registry Operators?	<p>It is much more efficient and cost effective for ICANN to perform the WHOIS checks/audits rather than the registry operators.</p> <p>ICANN is in the midst of implementing a WHOIS Online Accuracy Reporting System (“Accuracy Reporting System”) as a result of the adoption of the Board’s November 2012 resolution and the related Action Plan. As part of this initiative, ICANN is dedicating substantial resources to perform these checks and report on the associated accuracy levels.</p> <p>An RFP has been released by ICANN on May 16th &lt;<a href="https://www.icann.org/news/announcement-2014-05-19-en">https://www.icann.org/news/announcement-2014-05-19-en</a>&gt; to identify the various service providers and expertise needed to properly perform the WHOIS checks, including, for example, service providers capable of performing validation and verification of address, emails, telephone numbers and registrant contact details.</p> <p>As described in the Draft Implementation Plan for the Accuracy Reporting System, ICANN is deploying a standard methodology for determining accuracy of these data elements and will be developing a process whereby inaccurate WHOIS records will be forwarded to registrars for follow-up as appropriate. In addition, the process will also incorporate feedback to the ICANN Contractual Compliance Department in the event that any contractual enforcement issues arise.</p> <p>One of the advantages to ICANN performing these checks is that a consistent approach and methodology adopted will be adopted instead of experiencing different levels of WHOIS checks among the 1000+ new GTLDs.</p> <p>In addition, there should be an overall reduction of costs in the domain name ecosystem. If registry operators were required to perform these checks, each would likely need to acquire the services of commercial validation service providers to check the WHOIS contact details and would likely need to hire Staff to process the WHOIS checks &amp; interact with registrars. This additional burden, if spread over each registry operator,</p>
----	---	---

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		may result in increased costs for new gTLDs, making them less competitive with the legacy gTLDs.
2.	Does the NGPC believe ICANN has sufficient resources in place to conduct these audits, or will additional resources be necessary to conduct WHOIS checks across all Registry Operators?	ICANN is building the Accuracy Reporting System to be able to conduct WHOIS checks across all existing and new gTLD operators and all ICANN accredited registrars. The FY15 budget request incorporates anticipated funding for this project.
3.	Can the NGPC clarify the meaning of “periodic sampling” (e.g. how large will the sampling be, using what criteria, how often, etc.)? With a periodic sampling approach, will it be possible to identify/Registrars with the highest percentages of deliberately false, inaccurate or incomplete WHOIS records in previous checks?	<p>The methodology for periodic sampling to be included in the Accuracy Reporting System is being finalized through the work performed under the RFP issued by ICANN on 16 May 2014.</p> <p>The RFP solicits proposals for service providers to perform “Study Design and Delivery Services” to define the sampling methodology in order to produce statistically significant findings of various accuracy levels, using the proposed model developed by NORC and published in the Draft Implementation Plan.</p> <p>Taking into account recent WHOIS developments, such as the adoption of the new 2013 Registrar Accreditation Agreement (2013 RAA), the NORC model examines a WHOIS record for each of the validation perspectives highlighted in SSAC-58 [PDF, 490 KB], namely, syntactic, operational, and identity validation, and assigns a scoring methodology. These in turn will translate into a finding of accuracy labels, based on range of possibilities, such as:</p> <p style="padding-left: 40px;"><i>No Failure</i> <i>Minimal Failure</i> <i>Limited Failure</i> <i>Substantial Failure</i> <i>Full Failure</i></p> <p>which will be reported on a regular basis, and tracked over time. The model also describes a sampling methodology to ensure that a statistically significant number of records are examined to provide adequate geographic scope, and that enable a comparison of accuracy levels.</p> <p>The Accuracy Reporting System will enable a series of comparisons and</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		<p>reports to be published, including, for example:</p> <ul style="list-style-type: none"> <li>• Accuracy levels associated with new gTLDs and legacy gTLDs;</li> <li>• Accuracy levels associated with registrars under the 2013 Registrar Accreditation Agreement (RAA) versus the older versions of the RAA ;</li> <li>• Compliance levels with regards to the validation and verification of certain WHOIS contact data requirements, as listed in the Whois Accuracy Program Specification to the RAA;</li> <li>• Accuracy levels for registrars, registries and registrants located in each of the five ICANN Geographic Regions; and</li> <li>• Ranking of each ICANN accredited registrar and gTLD registry, based on reported accuracy levels.</li> </ul>
4.	<p>Will ICANN circulate/make publicly available to the community, detailed statistical reports of how inaccurate WHOIS records were identified and resolved?</p>	<p>The Accuracy Reporting System is being designed to publish detailed statistical reports at regularly defined intervals through the WHOIS website.</p> <p>Although the format of these reports has not been finalized, these will likely include summary information regarding the levels of inaccuracy detected and forwarded to registrars for follow-up.</p>
5.	<p>What steps does the NGPC think are needed to ensure inaccurate or incomplete WHOIS records are addressed? Will Registry Operators take steps to notify Registrars of inaccurate or incomplete WHOIS records? If so, will this notification trigger an obligation from the Registrar to solicit accurate and complete information from the Registrant?</p>	<p>The process identified above is not likely to require the involvement of registries, as it is envisioned that ICANN will directly forward the inaccuracies to registrars for follow-up.</p> <p>ICANN is currently consulting with registrars and the broader ICANN Community to define the process by which inaccurate records are forwarded to registrars, resolved, and re-checked by the Accuracy Reporting System.</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

**Safeguard 3** pertains to Security Checks undertaken by Registry Operators to periodically analyze whether domains in its gTLD are being used for threats to security, such as pharming, phishing, malware and botnets. While the NGPC has incorporated aspects of Safeguard 3 into the Public Interest Commitment Specification 11, it also calls on ICANN to seek “community participation” to develop a framework for Registry Operators to respond to identified security risks that pose an actual risk of harm. Pending the development of such a framework, it is not clear whether Registry Operators are obliged to notify a Registrar to take immediate actions in response to such security threats (including suspending the domain name in appropriate situations).

1.	How does ICANN define “immediate action;” what precise timeframe constitutes “immediate action”?	<p>In the Beijing Communiqué, the GAC advised, “While respecting privacy and confidentiality, Registry operators will periodically conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. If Registry operator identifies security risks that pose an actual risk of harm, Registry operator will notify the relevant registrar and, if the registrar does not take immediate action, suspend the domain name until the matter is resolved.” (See GAC Register #2013-04-11-Safeguards-3)</p> <p>The NGPC adopted a proposal to implement the safeguards. (See <a href="http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf">http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf</a>). The NGPC directed staff to include a provision in the New gTLD Registry Agreement to require registry operators to periodically conduct security checks, but the contract language adopted purposefully excluded the specific details for how the security checks should be conducted so that the community could help develop the parameters for conducting the security checks.</p> <p>The NGPC contemplated that ICANN would solicit the community to develop a framework for registry operators to respond to the identified security risks. Conferring the GAC would be included as part of the process.</p> <p>The framework to be developed by the community could include consideration of appropriate timeframes to respond to security risks.</p>
2.	How does ICANN define “security risk”?	The term “security threat” is used in Specification 11, Section (3)(a),

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		followed by non-exhaustive list of examples of common security threats, such as, pharming, phishing, malware and botnets.
3.	How does ICANN define “harm”?	As noted above, the NGPC contemplated that ICANN would solicit the community to develop a framework for registry operators to respond to the identified security risks. The framework to be developed by the community could include consideration of identifying security risks that pose an actual risk of harm.
4.	What is the status of the NGPC’s plan to develop a framework for Registry Operators to respond to identified security risks that pose an actual risk of harm?	During the ICANN meeting in London, ICANN will begin soliciting input from the community on the development of a proposed framework for conducting security checks and will analyze the responses and communicate next steps, including opening a public comment period.
5.	In the interim before an agreed framework is developed, how does ICANN intend to address such security threats?	Any Registry Operator signing the New gTLD Registry Agreement is obligated to conduct a technical analysis to assess whether domains in the TLD are being used to perpetuate security threats. (See Specification 11, Section 3.b.) The framework referenced in the question, is being developed to provide more specific implementation guidance and best practices in an effort to assist Registry Operators to comply with contractual requirements.
6.	Will Registry Operators be expected or obliged to notify a Registrar to take immediate action in response to a security threat that poses an actual risk of harm?	As required by the New gTLD Registry Agreement (Specification 11, Section 3.a), Registry Operators must include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders 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. Additionally, there must be consequences for such activities (consistent with applicable law and any related procedures), including suspension of a domain name.

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

**Safeguard 5** addresses Complaint Mechanisms, to ensure that Registry Operators provide a means by which complaints can be submitted related to: WHOIS data inaccuracy, trademark or copyright infringement, counterfeiting, fraudulent or deceptive practices, the use of malware, botnets, phishing, piracy, or other unlawful activities. The NGPC has incorporated this Safeguard in the Base Registry Agreement (e.g. Section 2.8, Specification 6, section 4.1). It is not clear, however, whether Registry Operators are required to respond to complaints from sources other than governments, law enforcement or other quasi-governmental entities.

1.	What mechanisms will be used by Registry Operators for taking complaints from sources other than government entities (e.g. victims)?	The current version of the contract obligates Registry Operators to take complaints from law enforcement, governmental, and quasi-governmental entities. In addition, Registry Operators are required by the Registry Agreement to publish on their websites their accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD. (See Registry Agreement Specification 6, Section 4.1)
2.	How will inaccurate WHOIS information be corrected? Will Registry Operators be responsible for ensuring that Registrars require Registrants to correct inaccurate WHOIS information?	<p>Inaccurate WHOIS information could be corrected through the WHOIS Inaccuracy Complaint System (the “System”). As part of the System, Internet users are able to submit a complaint to ICANN regarding incomplete or incorrect WHOIS data, including privacy or proxy contact information. The complaint is then forwarded to the sponsoring registrar, who must take reasonable steps to investigate and correct inaccurate data.</p> <p>The 2013 Registrar Accreditation Agreement (“2013 RAA”) also contains provisions addressing inaccurate WHOIS information. Under Section 3.7.7.2, it is a material breach of the contract between the Registered Name Holder and a Registrar if the Registered Name Holder willfully provides inaccurate or unreliable WHOIS information, or willfully fails to update information provided to Registrar. Such a failure can serve as the basis for suspension and/or cancellation of the Registered Name registration.</p> <p>A registrar under the 2013 RAA also has a role to play. If a registrar is notified of an inaccuracy in the contact information associated with a Registered Name sponsored by registrar, the registrar must take reasonable steps to investigate and correct that claimed inaccuracy. (See 2013 RAA</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		section 3.7.8 and the WHOIS Program Specification).
3.	What constitutes reasonable steps for the Registry to investigate and respond to any reports from law enforcement, governmental and quasi-governmental bodies?	<p>The term “reasonable steps” is not defined within the Registry Agreement. Precisely what constitutes reasonable steps to investigate and respond to reports from law enforcement, governmental and quasi-governmental bodies will vary depending on the circumstances. At a minimum, “reasonable steps” to investigate a reported inaccuracy should include promptly transmitting to the registrant the “inquiries” concerning the accuracy of the data that are suggested by the 2013 RAA Subsection 3.7.7.2. The inquiries should be conducted by all commercially practicable means available to the registrar: by telephone, e-mail, and postal mail.</p> <p>ICANN previously published an advisory on what may constitute “reasonable steps” with respect to a registrar’s obligation to correct inaccurate data pursuant to the Registrar Accreditation Agreement. While this advisory arises in a different context, there may be similarities to understanding what may constitute reasonable steps in the context of the question presented. A copy of the advisory is available here: <a href="http://www.icann.org/en/news/announcements/advisory-10may02-en.htm">http://www.icann.org/en/news/announcements/advisory-10may02-en.htm</a>.</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

<b>With regard to strings falling under Category 1 advice, we are seeking further clarity from the NGPC on the following:</b>		
1.	Is it the NGPC’s intention to create a separate base Registry Agreement for those Registry Operators whose strings fall under Category 1? Or does the NGPC expect such Registry Operators to incorporate the Category 1 PIC Spec into their specific Registry Agreement?	<p>The applicable Public Interest Commitments to address the Category 1 Safeguard advice are included in the base Registry Agreement for a string listed in the Category 1 Safeguard Advice. Based on the <a href="#">implementation framework</a> adopted by the ICANN Board New gTLD Program Committee on 5 February 2014, all Registry Agreements for Category 1 strings classified as “Regulated Sectors/Open Entry Requirements in Multiple Jurisdictions” are required to have three additional safeguards, and Category 1 strings classified as “Highly-regulated sectors/ Closed Entry Requirements in Multiple Jurisdictions” are required to have eight additional safeguards.</p> <p>For example, compare Specification 11 of the <a href="#">Registry Agreement for .ABOGADO</a>, which includes the eight additional Category 1 Safeguards because it is a string classified in the “Highly-regulated sectors/ Closed Entry Requirements in Multiple Jurisdictions” in the implementation framework to Specification 11 of the <a href="#">Registry Agreement for .GREEN</a>, which includes three additional Category 1 Safeguards because it is a string classified in the “Regulated Sectors/Open Entry Requirements in Multiple Jurisdictions” in the implementation framework.</p>
2.	In amending the GAC’s advice that Registry Operators verify and validate a domain name registrant’s credentials to a requirement that such registrants need only “represent” that they have such credentials, has the NGPC considered other measures to prevent consumer fraud and deception that could occur through false representations?	<p>Before implementing the GAC’s advice, on 23 April 2013, ICANN initiated a public comment forum to solicit input on how the NGPC should address GAC advice regarding safeguards applicable to broad categories of new gTLD strings <a href="http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm">http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm</a>. The Beijing Communiqué generated significant interest from the community and resulted in many comments, which the NGPC considered in formulating its response to the GAC advice.</p> <p>Overall, the NGPC adapted the language of the Category 1 safeguards as appropriate to meet the spirit and intent of the GAC’s Category 1 Safeguard Advice in a manner that allowed the safeguards to be implemented as public interest commitments in Specification 11 of the New gTLD Registry Agreement.</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		<p>When developing the framework to implement the Category 1 Safeguards, the NGPC considered whether implementation of the Safeguards #6 and #7 as originally drafted could potentially change the nature of some new gTLDs from being open to uses that are not regulated into restricted TLDs open only to registrants that can prove their status or credentials. In adopting the implementation framework, the NGPC noted that implementation would potentially discriminate against users in developing nations whose governments do not have regulatory bodies or keep databases which a registry/registrant could work with to verify credentials, and would potentially discriminate against users in developed nations whose governments have developed different regulatory regimes.</p> <p>The language adopted in Specification 11 was developed to address these concerns. As an initial matter, the registrant would be required to make an attestation that the registrant processes any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD string. The registrant is also required to report any material changes to the validity of their authorizations. This provision provides the registrant the opportunity to provide this information because it is better positioned to do so. If the registry operator receives complaints about the authenticity of the licenses or credentials, the registry operator is obligated to consult with the relevant national supervisory authorities, or their equivalents regarding the authenticity.</p> <p>It is also worth noting that fraud and consumer protection issues are within the ambit of government regulatory bodies and administrative agencies, and such issues may be addressed by governments as appropriate apart from the public interest commitments in the New gTLD Registry Agreement.</p>
3.	How will ICANN prevent Category 1 registrants (i.e., those associated with market sectors that have clear and/or regulated entry requirements) that lack the	As previously noted, the registrant would be required to make an attestation that the registrant processes any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD string. If the registry operator receives complaints about the

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

	proper credentials/licenses from doing business with the public under the guise of the Category 1 strings?	authenticity of the licenses or credentials, the registry operator is obligated to consult with the relevant national supervisory authorities, or their equivalents regarding the authenticity. Aside from the remedies provided in the New gTLD Registry Agreement, governmental agencies and bodies that address fraud and consumer protection could choose to address such issues that may arise.
4.	How will ICANN ensure that Registrants report changes regarding the validity of their licenses/credentials?	As provided in Specification 11, the registrant would be required (pursuant to the agreement between the registrant and the registrar) to make an attestation that the registrant processes any necessary authorizations, charters, licenses and/or other related credentials for participation in the sector associated with the TLD string. The registrant is also required to report any material changes to the validity of their authorizations. If the registry operator receives complaints about the authenticity of the licenses or credentials of the registrant, the registry operator is obligated to consult with the relevant national supervisory authorities, or their equivalents regarding the authenticity.
5.	<p>Has the NGPC considered the greater risks of fraud and deception that will occur as a result of failing to implement the GAC's:</p> <ul style="list-style-type: none"> <li>• the validation and verification requirements;</li> <li>• the requirement to consult with relevant authorities in case of doubt about the authenticity of credentials; and</li> <li>• the requirement to conduct periodic post-registration checks to ensure that Registrants' continue to possess valid credentials and generally conduct their activities in the interests of the consumers they serve</li> </ul>	<p>In adopting the framework to implement the GAC's Category 1 Safeguard Advice, the NGPC had to balance many competing positions, including weighing the relative advantages and challenges associated with implementing the advice in different ways. On balance, the language adopted in Specification 11 was developed to address all of the completing concerns in a way that respected the spirit and intent of the GAC's advice.</p> <p>As previously highlighted, on 23 April 2013, ICANN initiated a public comment forum to solicit input on how the NGPC should address GAC advice regarding safeguards applicable to broad categories of new gTLD strings <a href="http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm">http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm</a>. The Beijing Communiqué generated significant interest from the community and resulted in many comments, which the NGPC considered in formulating its response to the GAC advice.</p> <p>Additionally, the NGPC circulated its proposed implementation plan to the GAC on 29 October 2013 in advance of the ICANN Meeting in Buenos Aires.</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		<p>(<a href="https://www.icann.org/en/system/files/correspondence/crocker-to-dryden-3-29oct13-en.pdf">https://www.icann.org/en/system/files/correspondence/crocker-to-dryden-3-29oct13-en.pdf</a>) The proposed implementation plan was the subject of discussion between the meeting of the NGPC and the GAC in Buenos Aires, and the Buenos Aires Communiqué noted that “The GAC welcomed the response of the Board to the GAC’s Beijing Communiqué advice on Category 1 and Category 2 safeguards. The GAC received useful information regarding implementation of the safeguards during its discussions with the New gTLD Program Committee.”</p>
6.	<p>Can the NGPC confirm whether the PIC Dispute Resolution Process (PICDRP) is the sole remedy available to regulators or industry self-regulators to rectify fraudulent registrations in strings representing regulated sectors, and if so, will the NGPC either reconsider its proposed approach or develop a faster remedy to mitigate harm to consumers?</p>	<p>The PIC Dispute Resolution Process (PICDRP) is not the sole remedy available to regulators or industry self-regulators to rectify fraudulent registrants in strings representing regulated sectors, who may pursue remedies available through their own enforcement and/or administrative actions. The PICDRP provides one contractual remedy that is available under the Registry Agreement between ICANN and a registry operator.</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

<b>With regard to Category 2 safeguards, we are seeking further clarity on the following:</b>		
1.	For those Registry Operators affirmatively seeking exclusive registration policies, how does the NGPC intend to assess such Operators' assertions of serving the public interest?	The NGPC is preparing an approach and timeline as a path forward to address the remaining 12 applications which have provided information regarding how their TLDs serve the public interest.
2.	Has the NGPC considered that transparency alone might not only be insufficient to deter unduly preferential or discriminatory registration policies, but it will be equally difficult for anyone seeking redress to meet the standard of harm required in the PICDRP? In other words, if Specification 11 Section C is limited to a transparency commitment, then the harm stemming from discriminatory registration policies that are publicized cannot be amended or corrected through a PICDRP.	<p>Before implementing the GAC's advice, on 23 April 2013, ICANN initiated a public comment forum to solicit input on how the NGPC should address GAC advice regarding safeguards applicable to broad categories of new gTLD strings <a href="http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm">http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm</a>. The Beijing Communiqué generated significant interest from the community and resulted in many comments, which the NGPC considered in formulating its response to the GAC advice.</p> <p>Overall, the NGPC adapted the language of the Category 1 safeguards as appropriate to meet the spirit and intent of the GAC's Category 1 Safeguard Advice in a manner that allowed the safeguards to be implemented as public interest commitments in Specification 11 of the New gTLD Registry Agreement.</p>
3.	Will ICANN monitor Change Requests made by those applicants that claim they are moving from a closed to an open environment?	<p>Yes, ICANN is monitoring the change requests for all applicants named in GAC Category 2 Safeguard advice. Applicants who originally indicated that they intended to impose exclusive registry access for a generic string, but no longer wish to impose exclusive registry access must submit a change request to their application. (The applicants had until 21 March 2014 to submit a change request.)</p> <p>After the change request is approved, the applicant is required to submit a statement confirming that it does not intend to operate the applied-for TLD as an exclusive access registry. The applicant is also required to execute the Registry Agreement, which contains the mandatory PIC requirements applicable to all registries prohibiting a generic string from being operated as an exclusive TLD. This requirement is mandatory and not subject to</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		sunset. This commitment is a contractual requirement, as described above. This contractual obligation can and will be enforced by ICANN, via the Contractual Compliance Department and, as applicable, through the Public Interest Commitment Dispute Resolution Procedure (PICDRP).
--	--	--

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

<b>Public Interest Commitment Dispute Resolution Process (PICDRP):</b>		
1.	In the case of clearly deficient PICs, will ICANN formally require applicants to restate their PICs or address their inconsistencies?	<p>A Registry Agreement for the New gTLD Registry Program may contain two forms of contractually binding public interest commitments. In February 2013, ICANN provided applicants with the opportunity to make public interest commitments based on statements made in their applications and/or additional public interest commitments which were not included in their applications but to which they intend to commit. These commitments were voluntarily made by the applicants, and were published for review and comment by the community on 5 March 2013. These PICs are incorporated into Specification 11 of the Registry Agreement and are binding and enforceable contractual provisions.</p> <p>The second form of PICs are those PICs developed by the NGPC to implement advice issued by the GAC on the New gTLD Program. These PICs are standardized language, and are incorporated into Specification 11 of the Registry Agreement. Like the PICs voluntarily submitted by applicants, the PICs developed by the NGPC also are binding and enforceable contractual provisions.</p>
2.	Will ICANN turn PICs into real binding commitments not subject to unilateral modification or revocation by the applicant?	<p>Commitment made through PICs submitted by applicants, as well as PICs developed by the NGPC to address and implement the GAC's Category 1 and 2 Safeguard advice are incorporated into Specification 11 of the Registry Agreement and become binding contractual terms of the Registry Agreement, subject to enforcement through the PICDRP and ICANN Contractual Compliance.</p> <p>PICs, like other portions of the Registry Agreement, are not subject to unilateral modification or revocation. To change or amend a PIC, a Registry Operator would be subject to amendment procedures established in the Registry Agreement, which could include a public comment period and Board approval.</p> <p>Some applicants submitted voluntary PICs which include an expiration or</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		<p>sunset date. As previously noted, these PICs were posted for public comment. These conditions have been incorporated into Specification 11 and apply only to the voluntary PICs submitted by the applicant.</p>
3.	<p><b>Timeframe for consideration of a PIC Spec complaint is unclear.</b> The PICDRP does not specifically detail the timeframes in which ICANN will review and enforce the results of PICDRP disputes. Based on time calculations derived from PICDRP document, it may take up to <b>105</b> days for a dispute resolution, in addition to the undefined time periods for ICANN to conduct preliminary review, time for ICANN to investigate itself or form a standing panel; and time for ICANN to impose remedial measure.</p>	<p>In general, the timeframe for consideration of a PIC complaint varies and depends on several factors. For example, after a PIC complaint is submitted to a registry operator, the registry operator may request a conference with the party who submitted the complaint, and the registry operator has up to 30 days to hold the conference and try to resolve the complaint. A registry operator could resolve the complaint in a few days, or it may take a longer period to reach agreement.</p>
4.	<p><b>Preliminary Review</b> (Section B.1.3): How long will ICANN take to complete preliminary review? No timetable has been provided. In certain cases, <i>e.g.</i>, botnets, malware, etc., time is of the essence.</p>	<p>ICANN has established standard process and turn-around time for managing reports. The standard service level agreement (SLA) for responding to a new report or complaint is 3 business days. ICANN notes that if the submission requires additional information, then a request is made to the Reporter, who has five business days to provide the information/records requested.</p>
5.	<p><b>Standing Panel</b> (Section B.3.3; B.4): When will ICANN make determination of investigating the report itself or handing it to the Standing Panel? What criteria will ICANN use to make this determination? Who will be on the Standing Panel? How long will ICANN take to choose members of the Standing Panel? Will it be ICANN staff, private industry, and government? How long will it take to institute Standing Panel?</p>	<p>ICANN is currently interviewing prospective panelists for the PICDRP Standing Panel. ICANN is interviewing candidates with experience in one or more of the following disciplines: trademark protection, international dispute resolution, judicial/legal, contract interpretation, licensing, cultural studies, sociological research, online content, DNS, and cyber-security. The goal is to have as many of these skill sets represented on the Panel as possible, across a diverse set of panelists, but this is dependent on the panelists. It is anticipated that the panelist selections will be made by late June, mid-July and ICANN will work to enter into agreements with the Panelists thereafter.</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		The purpose of the Standing Panel is to refer PICDRP reports that are on topics outside of ICANN staff's expertise and scope to a panel of experts with specialize in those topics. The Panelists will be individuals who may have experience (past and/or present) working in private industry, the public sector, or both. After a decision is made to use the Standing Panel for a particular PIC complaint, it anticipated to take a few days to a week to institute the panelists that will work on the particular matter.
6.	<u>Standing for Law Enforcement and Appropriate Government Agencies to Report</u> : The PICDRP requires reporters of PIC violations to state how the reporters "have been harmed." This requirement seems to require the reporter itself to have suffered harm. Although law enforcement is not harmed, law enforcement is acting on behalf of the public, who have been harmed.	Section B.1.1 of the PICDRP states that "[a]ny person or entity that believes they have been harmed as a result of a Registry Operator's act or omission in connection with the operation of its gTLD that is non-compliant with its PICs may report such alleged non-compliance by the Registry Operator." ICANN will evaluate any and all complaints about non-compliance consistently, regardless of the complaining party.
7.	Will government entities or law enforcement have standing to raise concerns re: non-compliance with the Public Interest Commitments?	As noted above, ICANN will evaluate any and all complaints about non-compliance consistently, regardless of the complaining party.
8.	If government entities and law enforcement do have such standing to raise public policy related concerns, would this be cost-free?	There is not a cost associated with filing a complaint with the Contractual Compliance Department.
9.	How would law enforcement or other government entities (who act to protect the public) raise violations of the Public Interest Commitments?	To raise claims that a Registry Operator may not be complying with one or more of its Public Interest Commitments per Specification 11 of its Registry Agreement with ICANN, a complaining party should submit the standardized online form, available <a href="#">here</a> .  Aside from enforcement of the Public Interest Commitments, it should be noted that any violations of the PIC involving illegal conduct in connection with the use of the TLD may be directly referred to the registry operator, who per Article 2.8 of the RA, must respond to such reports and take reasonable steps to investigate.

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

10.	<p><b>Clerical Mistakes by Reporter:</b> Does the Reporter have a chance to correct clerical or incomplete data before it is dismissed by ICANN (B.1.1.2)?</p>	<p>A reporter has a chance to correct clerical or incomplete data before it is dismissed.</p>
11.	<p>ICANN vs. PICDRP? What will determine whether a dispute regarding the Public Interest Commitments is enforced via ICANN directly versus the PICDRP? (See B.2.3.3)</p>	<p>ICANN may elect to invoke the Standing Panel or undertake a compliance investigation with respect to one or more reports on a case-by-case assessment based on different criteria for example: the complexity of the alleged violations(s), potential impact on community, size of the registry operator, etc.</p> <p>Please note that contractual enforcement is always done by ICANN.</p>
12.	<p><b>No Final Resolution:</b> There appears to be a critical loophole in the PICDRP, in that there may be no resolution to the report of non-compliance. If the Registry Operator disagrees with the proposed remedial measure, they can invoke yet another alternate dispute resolution process (see B.4.4.6), all of which would occur after potentially more than 105 days has elapsed.</p>	<p>During the informal resolution process, the Registry Operator has the opportunity to propose remedial measures to address the PIC non-compliance issue. ICANN would evaluate the proposed remedial measures, and may request modifications to better protect the public interests.</p> <p>During the enforcement process, upon receipt of a notice of breach for non-compliance with the PIC, ICANN requests that the Registry Operator cure the breach by taking certain actions. Per Article 5 of the Registry Agreement, if the Registry Operator or ICANN disagree, it must attempt to resolve the dispute first through mediation (Article 5.1), then through arbitration (Article 5.2).</p>
13.	<p><b>Remedial Measures:</b> In the event that a Registry Operator fails to resolve its non-compliance, what would be the remedial measures that ICANN will consider and how long will ICANN take to determine the appropriate remedial measure? Under what circumstances would ICANN elect not impose a serious remedial measure? (B.4.4.5)</p>	<p>Specification 11 provides reasonably broad latitude for ICANN to fashion a remedy to address non-compliance with the PICs. Specifically, the Registry Agreement provides that “Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Agreement) following a determination by any PICDRP panel and to be bound by any such determination.”</p> <p>The Registry Operator has 30 days to cure the breach. The registry operator</p>

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		may be terminated if (i) thirty (30) days pass without curing ICANN’s notice of breach, (ii) an arbitrator determines that the registry operator is in fundamental and material breach of the covenants of Article 2.18, and (iii) ten (10) days pass without the registry operator complying with such determination and curing the breach.
14.	Repeat Offenders:  ICANN does not specify what sanctions (e.g. financial or otherwise) will be imposed on repeat offenders. (See B.5.5.4)	The potential sanctions that could be imposed on a repeat offender depend in part on whether the registry operator or a complaining/reporting party is the repeat offender. If the registry operator is found to be a repeat offender, ICANN may impose financial sanctions. If the complaining/reporting party is found to be a repeat offender, ICANN may bar future reporting of such party.

1.	<b>Auctions</b> Is ICANN able to provide more detailed information confirming that rules for auctions are consistent with its Bylaws, its not-for profit status, the objectives of the new gTLD Program and the Applicant Guidebook to promote competition, diversity, innovation and consumer choice?	<p>New gTLD Auctions as a last-resort mechanism for contention resolution were developed in accordance with is consistent with ICANN Bylaws and consistent with as well as 2007the GNSO 2007 New gTLD policy recommendations.</p> <p>The Applicant Guidebook (AGB) defined a “general introduction and preliminary” set of procedures including an ascending clock auction methodology and prescribed that a detailed set of Auction Rules would be made available prior to commencement of the auctions. Over the past eight months ICANN staff consulted with an experienced auction firm, Power Auctions LLC (Power Auctions), and with the ICANN community on the development of a set of detailed Auction Rules, as well as on the operational logistics to coordinate and execute auctions.</p> <p>In March 2014, after the conclusion of a public comment process, a set of Auction Rules was published. After further discussions during ICANN 49, the Auctions Rules were updated to address the remaining concerns of potential participants {<a href="http://newgtlds.icann.org/en/applicants/auctions/rules-03apr14-en.pdf">http://newgtlds.icann.org/en/applicants/auctions/rules-03apr14-en.pdf</a>}.</p>
----	---	---

**Annex 2**  
**NGPC Resolution 2014.06.06.2c**

		ICANN staff and Power Auctions took great care to ensure the Auction Rules were consistent with the descriptions of the auction procedures contained in the 4 June 2012 version of the AGB and that they incorporated the feedback of the community.
--	--	--

**New gTLD Program Committee Members,**

**Attached below please find Notice of the following New gTLD Program Committee Meeting:**

**6 June 2014 – NGPC Meeting at 13:00 UTC. This Committee meeting is estimated to last 2 hours and 30 minutes.**

**<http://www.timeanddate.com/worldclock/fixetime.html?msg=New+gTLD+Program+Committee+Meeting&iso=20140606T06&p1=137&ah=2&am=30>**

**Some other helpful time zones:**

**6 June 2014 – 6:00 a.m. PDT Los Angeles, CA**

**6 June 2014 – 9:00 a.m. EDT Washington, D.C.**

**6 June 2014 – 3:00 p.m. CEST Brussels**

#### **Main Agenda**

- 1. BGC Recommendations on .WINE & .VIN Reconsideration Requests**
- 2. GAC Advice regarding Community Views - .HEALTH and health-related TLDs**
- 3. GAC Advice Scorecard**
- 4. Possible Review Mechanism for Perceived Inconsistent String Confusion Objection Expert Determinations**
- 5. Name Collision Framework**
- 6. BGC Recommendation on Reconsideration Request 13-9, Amazon EU S.á.r.l.**

7. BGC Recommendation on Reconsideration Request 13-10,  
Commercial Connect, LLC
8. New gTLD Program Financial Update
9. AOB

**MATERIALS – [Once materials are available, you can find them here on BoardVantage.](#)**

**If you have trouble with access, please let us know and we will work with you to assure that you can use the BoardVantage Portal for this meeting.**

**If call information is required, it will be distributed separately.**

**If you have any questions, or we can be of assistance to you, please let us know.**

**John Jeffrey  
General Counsel & Secretary, ICANN  
[John.Jeffrey@icann.org](mailto:John.Jeffrey@icann.org) <[John.Jeffrey@icann.org](mailto:John.Jeffrey@icann.org)>  
<<mailto:John.Jeffrey@icann.org> <<mailto:John.Jeffrey@icann.org>>>**