

## Annex I

### NGPC Proposal for Implementation of GAC Safeguards Applicable to All New gTLDs

19 June 2013

The following is a draft proposal for how ICANN could implement the “GAC Safeguards Applicable to All New gTLDs.” This is an unapproved draft subject to further NGPC consideration.

#### 1. WHOIS Verification and Checks (GAC Register # 2013-04-11-Safeguards-1)

ICANN is concluding its development of a WHOIS tool that gives it the ability to check false, incomplete or inaccurate WHOIS data as the Board previously directed staff in Board Resolutions 2012.11.08.01 - 2012.11.08.02 to begin to “proactively identify potentially inaccurate gTLD data registration in gTLD registry and registrar services, explore using automated tools, and forward potentially inaccurate records to gTLD registrars for action; and 2) publicly report on the resulting actions to encourage improved accuracy.” <<http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm>>

Given these ongoing activities, ICANN (instead of Registry Operators) is well positioned to implement the GAC’s advice that checks identifying registrations in a gTLD with deliberately false, inaccurate or incomplete WHOIS data be conducted at least twice a year. To achieve this, ICANN will perform a periodic sampling of WHOIS data across registries in an effort to identify potentially inaccurate records. ICANN will also maintain statistical reports that identify the number of inaccurate WHOIS records identified. This undertaking by ICANN would not require ICANN to provide special certifications to Registry Operators certifying the accuracy of any WHOIS data. The WHOIS verification

and checks would be focused on the current version of WHOIS requirements, but would eventually broaden to include directory services.

## 2. Mitigating Abusive Activity (GAC Register # 2013-04-11-Safeguards-2)

ICANN will include a provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11)

<<http://newgtlds.icann.org/en/applicants/agb/base-agreement-specs-29apr13-en.pdf>>

obligating Registry Operators to 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, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

Paragraph 2 of the PIC Specification attached as Annex II includes language to implement the GAC advice. Because the Registry Operator does not have a direct contractual relationship with the Registered Name Holder, the language proposed in the PIC Specification would require the Registry Operator to include a provision in its Registry-Registrar Agreement, which in turn requires Registrars to include a provision in their Registration Agreements prohibiting Registered Name Holders from engaging in the abusive activity listed in the GAC advice.

## 3. Security Checks (GAC Register # 2013-04-11-Safeguards-3)

ICANN will include a provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) requiring Registry Operators periodically to 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. The provision will also require Registry Operators to maintain statistical reports

on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate.

Because there are multiple ways for a Registry Operator to implement the required security checks, ICANN will solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality. The language include in Paragraph 3 of the attached PIC Specification provides the 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 checks. This will permit Registry Operators to enter into agreements as soon as possible, while allowing for a careful and fulsome consideration by the community on the implementation details.

#### 4. Documentation (GAC Register # 2013-04-11-Safeguards-4)

As detailed in #1 above, ICANN will maintain statistical reports that identify the number of inaccurate WHOIS records identified as part of the checks to identify registrations with deliberately false, inaccurate or incomplete WHOIS data. Also, as detailed in #3 above, Registry Operators will be required to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate.

5. Making and Handling Complaints (GAC Register # 2013-04-11-Safeguards-5)

Registry Operators will be required to ensure that there is a mechanism for making complaints to the Registry Operator regarding malicious conduct in the TLD. Section 4.1 of Specification 6 of the proposed New gTLD Registry Agreement provides that, “Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquires related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.” Also, Section 2.8 of the proposed New gTLD Registry Agreement provides that a, “Registry Operator shall 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.”

ICANN operates the WHOIS Data Problem Reports System

<<http://www.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form>>, which is a mechanism for making complaints that WHOIS information is inaccurate.

6. Consequences (GAC Register # 2013-04-11-Safeguards-6)

As indicated in #2 above, ICANN will include a provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) obligating Registry Operators to 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, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

Consequences for the demonstrated provision of false WHOIS information are set forth in Section 3.7.7.2 of the 2013 RAA

<<http://www.icann.org/en/resources/registrars/raa/proposed-agreement-22apr13-en.pdf>>:

“A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.” Paragraph 1 of the proposed PIC Specification includes a requirement that Registry Operator will use only ICANN accredited registrars that are party to the 2013 RAA so that these consequences are contractually required.