Please see preliminary comments in-line, below, in blue.

GNSO Transfer Policy Review Policy Development Process Working Group (PDP WG) - Request for Early Input

To: ICANN Supporting Organizations / Advisory Committees / GNSO Stakeholder Groups / GNSO Constituencies

From: Transfer Policy Review PDP WG

Subject: Request for Early Input

---

30 June 2021

Dear Community Leader:

I am writing to you on behalf of the GNSO PDP WG that is tasked with reviewing the Transfer Policy and determining if changes to the policy are needed to improve the ease, security, and efficacy of inter-registrar and inter-registrant transfers. In accordance with GNSO policy development process requirements, we are seeking the written opinion on the topic from each Supporting Organization, Advisory Committee and GNSO Stakeholder Group / Constituency. While every Supporting Organization, Advisory Committee, and GNSO Stakeholder Group / Constituency has been invited to participate in the PDP, we are nonetheless also providing this opportunity to make a written submission for the PDP's consideration.

In order to ensure that this PDP can progress in a timely manner, we are requesting input within 35 days from today, i.e., **no later than 4 August 2021**. We do so because:

1) the working group will start substantive discussions immediately, so it is important for input to be timely to ensure that it is fully taken into account in the deliberations,

2) every ICANN Supporting Organization, Advisory Committee and GNSO Stakeholder Group / Constituency has been afforded the opportunity to participate in the working group so the opportunity for this early input is somewhat redundant, and

3) there will be additional opportunities for community input as the PDP progresses.

The working group's scope of work is defined through a series of questions presented in the working group's charter. These questions are organized under eight topic areas that will be considered by the working group in two phases. Currently, the working group is seeking input on the questions for phase 1, which focus on the following topics:

1. Gaining & Losing Registrar Form of Authorization ("FOA"), including items raised in the Expedited Policy Development Process Recommendation 27, Wave 1 Report as they relate to FOA requirements
2. AuthInfo Code Management
3. Change of Registrant, including items raised in the Expedited Policy Development Process Recommendation 27, Wave 1 Report as they relate to Change of Registrant

Please see attached for the list of questions. To the extent possible, you are requested to provide your responses in the attached document with responses provided to individual questions. It is not necessary to respond to every question and you are welcome to provide any other input that you deem helpful in facilitating the deliberations. At the same time, in order to support focused and organized deliberations on the phase 1 topics, input on the questions presented will be most valuable.

Please submit your response to gnso-secs@icann.org. Timely input will be incorporated into a summary document and provided to the working group. Input received after the due date may be introduced into the discussion by your SO/AC/SG/C representative, ICANN support staff, or me as the pertinent topic arises.

Thank you very much and I look forward to receiving your input.

On behalf of the PDP WG,

Roger Carney
PDP WG Chair

BACKGROUND

The Transfer Policy, formerly referred to as the Inter-Registrar Transfer Policy (IRTP), is an ICANN consensus policy governing the procedure and requirements for registrants to transfer their domain names from one registrar to another.

On April 22, 2019, ICANN Org delivered the Transfer Policy Status Report to the GNSO Council pursuant to Recommendation 18 of the Inter-Registrar Transfer Policy (IRTP) Part D PDP Working Group's Final Report. Recommendation 18 states, "[t]he Working Group recommends that contracted parties and ICANN should start to gather data and other relevant information that will help inform a future IRTP review team in its efforts."

During its meeting on September 19, 2019, the GNSO Council agreed to launch a call for volunteers for a Transfer Policy Review Scoping Team. The Scoping Team was tasked with advising the GNSO Council by providing recommendations on the approach to the review (for example, by initiating a new PDP), the composition of the review team or PDP working group, and the scope of the review and future policy work related to the Transfer Policy.

On April 6, 2020, the Transfer Policy Review Scoping Team delivered its Transfer Policy Review Scoping Paper to the GNSO Council for its consideration. The Scoping Team recommended that the GNSO Council instruct ICANN Policy staff to draft an Issues Report, outlining, et.al., the issues described in its Scoping Paper. On 23 June 2020, the GNSO Council voted to approve a motion requesting a Preliminary Issue Report, for delivery as expeditiously as possible, on the issues identified in the Transfer Policy Initial Scoping Paper, to assist in determining whether a PDP or series of PDPs should be initiated regarding changes to the Transfer Policy.

On 18 February 2021, The GNSO Council passed a resolution to initiate a two-phased PDP to review the Transfer Policy. The PDP working group is tasked with determining if changes to the policy are needed to improve the ease, security, and efficacy of inter-registrar and inter-registrant transfers.

Transfer Policy Review PDP WG

Questions for Community Input

Phase 1(a) Questions

The following topics will be considered under Phase 1(a):

- Gaining Registrar FOA and Losing Registrar FOA
- AuthInfo Code Management
- Rec. 27, Wave 1 Report (as it relates to FOA requirements)

a) **Gaining Registrar FOA and Losing Registrar FOA**

Gaining FOA

a1) Is the requirement of the Gaining FOA still needed? What evidence did the Working Group rely upon in making the determination that the Gaining FOA is or is not necessary to protect registrants?

Although apparently not necessary from a practical perspective, the Gaining FOA may have some utility as a means of evidencing a transfer.

a2) If the Working Group determines the Gaining FOA should still be a requirement, are any updates (apart from the text, which will likely need to be updated due to the gTLD Registration Data Policy) needed for the process? For example, should additional security requirements be added to the Gaining FOA (two-factor authentication)?

No comment.

a3) The language from the Temporary Specification provides, "[u]ntil such time when the RDAP service (or other secure methods for transferring data) is required by ICANN to be offered, if the Gaining Registrar is unable to gain access to then-current Registration Data for a domain name subject of a transfer, the related requirements in the Transfer Policy will be superseded by the below provisions…". What secure methods (if any) currently exist to allow for the secure transmission of then-current Registration Data for a domain name subject to an inter-registrar transfer request?

No comment.

a4) If the Working Group determines the Gaining FOA is no longer needed, does the AuthInfo Code provide sufficient security? The Transfer Policy does not currently require specific security requirements around the AuthInfo Code. Should there be additional security requirements added to AuthInfo Codes, e.g., required syntax (length, characters), two-factor authentication, issuing restrictions, etc.?

We are unaware of any evidence that AuthInfo Codes have been compromised, however if there are security concerns then 2FA and expiry times should be considered.

a5) If the Working Group determines the Gaining FOA is no longer needed, does the transmission of the AuthInfo Code provide for a sufficient “paper trail” for auditing and compliance purposes?

The mere provision of an AuthInfo Code is unlikely to provide a sufficient paper trail.

Additional Security Measures

a6) Survey respondents noted that mandatory domain name locking is an additional security enhancement to prevent domain name hijacking and improper domain name transfers. The Transfer Policy does not currently require mandatory domain name locking; it allows a registrar to NACK an inter-registrar transfer if the inter-registrar transfer was requested within 60 days of the domain name’s creation date as shown in the registry RDDS record for the domain name or if the domain name is within 60 days after being transferred. Is mandatory domain name locking an additional requirement the Working Group believes should be added to the Transfer Policy?

Mandatory domain name locking should not be introduced as it negatively impacts and impedes portability for registrants. Registrars should fully disclose their respective locking polices so as to enable informed consumer choices in the selection of a registrar. Registrars should be required to provide opt-outs to registrants in an obvious and automated manner.

Losing FOA

a7) Is the Losing FOA still required? If yes, are any updates necessary?

Although apparently not necessary from a practical perspective, the Losing FOA may have some utility as a means of evidencing a transfer.

a8) Does the CPH Proposed Tech Ops Process represent a logical starting point for the future working group or policy body to start with? If so, does it provide sufficient security for registered name holders? If not, what updates should be considered?

Good starting point.

a9) Are there additional inter-registrar transfer process proposals that should be considered in lieu of or in addition to the CPH TechOps Proposal? For example, should affirmative consent to the Losing FOA be considered as a measure of additional protection?

Transfer locks should be removable by the registrant.

b) **Auth-Info Code Management**

b1) Is AuthInfo Code still a secure method for inter-registrar transfers? What evidence was used by the Working Group to make this determination?

It appears secure in the absence of other evidence.

b2) The registrar is currently the authoritative holder of the AuthInfo Code. Should

this be maintained, or should the registry be the authoritative AuthInfo Code holder? Why?

Registrar should be authoritative holder.

b3) The Transfer Policy currently requires registrars to provide the AuthInfo Code to the registrant within five business days of a request. Is this an appropriate SLA for the registrar's provision of the AuthInfo Code, or does it need to be updated?

Should be instant.

b4) The Transfer Policy does not currently require a standard Time to Live (TTL) for the AuthInfo Code. Should there be a standard Time To Live (TTL) for the AuthInfo Code? In other words, should the AuthInfo Code expire after a certain amount of time (hours, calendar days, etc.)?

Yes. Should expire after period of time, such as 3 days, provided it is provided instantly.

Bulk Use of Auth-Info Codes

b5) Should the ability for registrants to request AuthInfo Codes in bulk be streamlined and codified? If so, should additional security measures be considered?

Ideally bulk requests should be streamlined. But in their absence registrars do provide this service, albeit manually.

b6) Does the CPH TechOps research provide a logical starting point for future policy work on AuthInfo Codes, or should other options be considered?

Yes.

b7) Should required differentiated control panel access also be considered, i.e., the registered name holder is given greater access (including access to the auth code), and additional users, such as web developers would be given lower grade access in order to prevent domain name hijacking?

Yes, ideally.

c) **Wave 1, Recommendation 27, as it relates to FOA**

c1) How should the identified issues be addressed?

In WG.

c2) Can the FOA-related Transfer Policy issues (identified in paragraphs 5 and 9 of

Wave 1 Report),[1] as well as the proposed updates to the Gaining and Losing FOAs, be discussed and reviewed during the review of FOAs?

Yes.

Phase 1(b) Questions

The following topics will be considered under Phase 1(b):

- Change of Registrant
- Rec. 27, Wave 1 Report (as it relates to Change of Registrant)

d) **Change of Registrant**

Change of Registrant – Overall Policy

d1) According to the Transfer Policy Review Scoping Team Report, the Change of Registrant policy "does not achieve the stated goals" and "is not relevant in the current & future domain ownership system." To what extent is this the case and why? Are the stated goals still valid? If the Change of Registrant policy is not meeting the stated goals and those goals are still valid, how should the goals be achieved?

The explanations for why the Change of Registrant Policy does not meet its stated goals is adequately explained in the Scoping Team Report, namely:

"The COR process is burdensome and confusing to registrants. Registrant point-of-view: When the domain exists within a single registrar, why should a material change of the registrant trigger a "transfer" process action such as "Change of Registrant" and lock the domain for 60 days? When transferring domains between registrars, registrants often "clean up" their contact data before the registrar transfer. The COR process hinders this immensely. Change of Registrant is a completely different topic than a transfer between Registrars and should be addressed in separate efforts. The scenario where a Change of Registrar occurs simultaneously with a Change of Registrant should be addressed as a discrete use case since this occurs frequently in the domain aftermarket. A standalone policy should be considered for this, and the policy should also consider the aforementioned use case where a Change of Registrar occurs simultaneously with a Change of Registrant."

d2) Data gathered in the Transfer Policy Status Report indicates that some registrants find Change of Registrant requirements burdensome and confusing. If the policy is retained, are there methods to make the Change of Registrant policy simpler while still maintaining safeguards against unwanted transfers?

[1] https://mm.icann.org/pipermail/council/attachments/20200219/94112f0f/Rec27-Wave1-Updated-14feb20-0001.pdf

The Transfer Policy is nearly incomprehensible to those that are legally trained, let alone the average registrant or business owner. Moreover, it is often misunderstood by ICANN, registrars and registrants. Change of Registrant requirements should be rewritten and redesigned from the ground up in a comprehensible and user friendly manner, with secure portability of domain names being the priority and

d3) The Transfer Policy Review Scoping Team Report suggests that there should be further consideration of establishing a standalone policy for Change of Registrant. According to the Scoping Team, the policy should take into account the use case where a Change of Registrar occurs simultaneously with a Change of Registrant. To what extent should this issue be considered further? What are the potential benefits, if any, to making this change? To what extent does the policy need to provide specific guidance on cases where both the registrar and registrant are changed? Are there particular scenarios that need to be reviewed to determine the applicability of COR?

- Gaining Registrar allows a new customer to input the Registrant information when requesting an inbound inter-registrar transfer. The information entered by the customer does not match Registration Data available in the Whois display.
- In the case of "thin" domain names, the Gaining Registrar obtains information from the Registry.

If it is determined that the Change of Registrant policy should be retained and modified, the following specific areas may be appropriate for further review.

A stand alone policy should be seriously considered further. This will increase the ability for registrants and registrars alike to comprehend the policy.

Registrants look for security and portability amongst other important factors when selecting a registrar. Locks can sometimes play an important role in securing a valuable domain name. When a registrar locks a domain name upon changing a registrant or changing registrars that may give the registrant time to notice an unauthorized change and better enable the registrar to assist in recovering the domain name, for example via the Registrar Transfer Dispute Resolution Policy. Locking a domain name may also assist a registrar in ensuring that it gets paid for the domain name prior to it being transferred to another registrar.

Nevertheless, locks are not the only kind of security available to registrars and registrants. Security measures such two-factor authentication (2FA) can be implemented by registrars in order to avoid unauthorized transfers of domain names in the first place and have been proven to be very effective in avoiding domain name theft.

Where locks are imposed as a security mechanism it is important for registrars and registrants alike to be aware of when and why a domain name may be locked. There are widespread misconceptions about who requires locks and when they are mandatory. From a careful review of ICANN's Transfer Policy – which is a very confusing document even for experienced lawyers to comprehend – it is apparent that some registrars themselves are unclear on when they are required to impose a lock and when they are not. Similarly, many registrants are unaware that ICANN policy is generally

permissive when it comes to imposing locks – leaving it to the discretion of the registrar in many cases.

60-Day Lock

d4) Survey responses and data provided by ICANN's Global Support Center indicate that registrants do not understand the 60-day lock and express frustration when it prevents them from completing an inter-registrar transfer. Does the 60-day lock meet the objective of reducing the incidence of domain hijacking? What data is available to help answer this question? Is it the 60-day lock the most appropriate and efficient mechanism for reducing the incidence of hijacking? If not, what alternative mechanisms might be used to meet the same goals? Are there technical solutions, such as those using the control panel or two-factor authentication, or other alternatives that should be explored?

Absent evidence that 60-day locks provide security that cannot be provided by less intrusive and burdensome means, it should not be maintained as is. Registrants should be able to easily and securely opt out of it.

d5) Survey responses and data provided by ICANN's Global Support Center and Contractual Compliance Department indicate that registrants have expressed significant frustration with their inability to remove the 60-day lock. If the 60-day lock is retained, to what extent should there be a process or options to remove the 60-day lock?

Registrants should be able to easily and securely opt out of it.

d6) Due to requirements under privacy law, certain previously public fields, such as registrant name and email may be redacted by the registrar. Is there data to support the idea that the lack of public access to this information has reduced the risk of hijacking and has therefore obviated the need for the 60-day lock when underlying registrant information is changed?

Anecdotally there is some evidence.

d7) In its survey response, the Registrar Stakeholder Group indicated that the 60-day lock hinders corporate acquisitions, consolidations, and divestitures of large lists of domains to new legal entities. To what extent should this concern be taken into consideration in reviewing the 60-day lock?

This is a serious concern that must be addressed.

d8) If the policy is retained, are there areas of the existing policy that require clarification? For example, based on complaints received by ICANN Contractual Compliance, the following areas of the policy may be appropriate to review and clarify:

- There have been different interpretations of footnote 4 in the Transfer Policy, which states: "The Registrar may, but is not required to, impose restrictions

on the removal of the lock described in Section II.C.2. For example, the Registrar will only remove the lock after five business days have passed, the lock removal must be authorized via the Prior Registrant's affirmative response to email, etc." Is the language in footnote 4 sufficiently clear as to whether registrars are permitted to remove the 60-day lock once imposed under the existing policy? If not, what revisions are needed?

- Should additional clarification be provided in Section II.C.1.3, which addresses how the information about the lock must be provided in a clear and conspicuous manner? Does the policy contemplate enough warning for registrants concerning the 60-day lock where they are requesting a COR?
- Should clarification be provided in Section II.C.2 that the option to opt-out is provided only to the Prior Registrant? For example, would the following revision be appropriate: "The Registrar must impose a 60-day inter-registrar transfer lock following a Change of Registrant, provided, however, that the Registrar may allow the **Prior Registrant** to opt out of the 60-day inter-registrar transfer lock prior to any Change of Registrant request."?

The whole things needs a 'page 1 rewrite' to make it comprehensible.

Change of Registrant – Privacy/Proxy Customers

d9) A Change of Registrant is defined as "a Material Change to any of the following: Prior Registrant name, Prior Registrant organization, Prior Registrant email address Administrative Contact email address, if there is no Prior Registrant email address." Registrars have taken the position that the addition or removal to a privacy/proxy service is not a Change of Registrant; however, there is not currently an explicit carve-out for changes resulting from the addition or removal of privacy/proxy services vs. other changes. To what extent should the Change of Registrant policy, and the 60-day lock, apply to underlying registrant data when the registrant uses a privacy/proxy service?

- Registrars have identified a series of specific scenarios to consider in clarifying the application of COR policy requirements where the customer uses a privacy/proxy service.[2] Are there additional scenarios that need to be considered that are not included in this list?

Material changes should not necessarily result in a lock and the definition of material needs to be revisited.

d10) Should the policy be the same regardless of whether the registrant uses a privacy service or a proxy service? If not, how should these be treated differently?

No comment.

d11) Are notifications provided to privacy/proxy customers regarding COR and changes to the privacy/proxy service information sufficient? For example, should

[2] See Appendix A to the 1 December 2016 letter from the GNSO Council to the ICANN Board: https://gnso.icann.org/sites/default/files/file/field-file-attach/bladel-to-crocker-01dec16-en.pdf

there be additional notifications or warnings given to a privacy/proxy customer if the privacy/proxy service regularly changes the privacy/proxy anonymized email address?

Yes.

Designated Agent

d12) In its survey response, the Registrar Stakeholder Group indicated that, "There is. . . over-use of the Designated Agent, which has basically circumvented the policy." To what extent is this the case? What is the impact?

The Policy should be adapted to circumvent the need for this.

d13) If the Designated Agent function is not operating as intended, should it be retained and modified? Eliminated?

Possibly eliminated.

d14) Are there alternative means to meet the objectives of Designated Agent role?

d15) Based on complaints received by ICANN's Contractual Compliance Department, there appear to be different interpretations of the role and authority of the Designated Agent. If the Designated Agent function remains, should this flexibility be retained? Does the flexibility create the potential for abuse?

Registrants should be able to approve all changes.

d16) If the role of the Designated Agent is to be clarified further, should it be narrowed with more specific instructions on when it is appropriate and how it is to be used?

- Should the Designated Agent be given blanket authority to approve any and all CORs? Or should the authority be limited to specific COR requests? Does the authority to approve a COR also include the authority to request/initiate a COR without the Registered Name Holder requesting the COR?

Additional Questions

d17) The Registrar Stakeholder Group recommended the following in its survey response: "For a Change of Registrant, both the gaining and losing registrants should be notified of any requests, and should have the option accept or reject, over EPP notifications." Should this proposal be pursued further? Why or why not?

This is satisfactory.

e) **Wave 1, Recommendation 27, as it relates to Change of Registrant**

e1) How should the identified issues be addressed?

See above.

e2) Can the Change of Registrant-related issue (identified in paragraph 6 of the Wave 1 report) be discussed and reviewed during the review of the Change of Registrant Process?

Yes.