ICANN | GNSO

Generic Names Supporting Organization

Final Issue Report on a Policy Development Process to Review the Transfer Policy

Status of This Document

This is the Final Issue Report on a Policy Development Process to Review the Transfer Policy as requested by the GNSO Council. This report is published following the closure of the public comment forum on the Preliminary Issue Report, which was published on 12 October 2020.

Summary

This report is submitted to the GNSO Council in response to a request received on 24 June 2020. On 24 June 2020, the GNSO Council passed a motion, requesting ICANN's Policy Support Staff to draft a Preliminary Issue Report on the issues identified in the Transfer Policy Review Initial Scoping Paper, which was requested as part of the GNSO Council's review of the Transfer Policy. The objective of the Preliminary Issue Report was for ICANN org to assess all relevant issues related to the GNSO Council request, and, following Community Input during the Public Comment phase, to recommend a course of action to the GNSO Council. It remains the GNSO Council's prerogative to either follow ICANN org recommendations or to pursue alternative action.

Table of Contents

1 Executive Summary

1.1. Discussion of the issue

The Transfer Policy, formerly referred to as the Inter-Registrar Transfer Policy (IRTP), is an ICANN consensus policy that went into effect on 12 November 2004. The policy governs the procedure and requirements for registrants to transfer their domain names from one registrar to another, also referred to as an inter-registrar transfer. The goal of the Transfer Policy was to provide for enhanced domain name portability, resulting in greater consumer and business choice and enabling registrants to select the registrar that offers the best services and price for their needs.

On April 22, 2019, ICANN Org delivered the Transfer Policy Status Report to the GNSO Council. ICANN Org delivered the Transfer Policy Status Report pursuant to Recommendation 17 of the Inter-Registrar Transfer Policy (IRTP) Part D PDP Working Group's Final Report, which provides, "[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, comprised of interested and knowledgeable GNSO Members that were tasked with advising the GNSO Council by providing recommendations on the following:

- approach to the review (for example, by initiating a new PDP);
- composition of the review team or PDP working group, and
- 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.

This Final Issue Report addresses eight issues associated with the Transfer Policy, seven of which were specifically identified by the Transfer Policy Review Scoping Team.
The eight issues addressed are:

a) Gaining & Losing Registrar Form of Authorization ("FOA")
b) Authcode Management
c) Change of Registrant
d) Transfer Emergency Action Contact ("TEAC")
e) Transfer Dispute Resolution Policy ("TDRP")
f) Reversing/NACKing Transfers
g) ICANN-Approved Transfers
h) EPDP Rec. 27

Section 3 of this Report explores the above-referenced issues individually and provides references to documents and processes that could inform future policy work.

1.2. Staff recommendation

ICANN org has confirmed that the proposed issues are within the scope of the GNSO's Policy Development Process (see Section 2).

ICANN org has confirmed that the proposed issues are within the scope of the GNSO's Policy Development Process and the GNSO (see section 5).

The Transfer Policy Status Report provided a foundation to review the history and underlying goals of Transfer Policy, the five policy development processes that sought to improve the Transfer Policy, and associated metrics on the Transfer Policy. The Transfer Policy Review Scoping Team's review of the Transfer Policy Status Report provided recommended topics for consideration, which served as the basis for analysis within the scope of this Issue Report and is expected to be the focus of the recommended multi-phased PDP.

A successful outcome of this PDP is critical to addressing the issues identified by the Transfer Policy Review Scoping Team and confirmed in this Issue Report. ICANN org therefore recommends that a multi-phased PDP proceed by carefully considering the recommended subjects of the Transfer Policy Review Scoping Team and work constructively toward new or modified policy recommendations for the Transfer Policy.

1.3. Next steps

In accordance with the GNSO Policy Development Process, ICANN org published a Preliminary Issue Report for public comment in order to allow for community input on additional information that may be missing from the Preliminary Issue Report, or the correction or updating of any information in the Preliminary Issue Report. In addition, the public comment period allowed for members of the ICANN Community to express their views to the GNSO Council on whether or not to initiate a PDP. Following review of the public comments received, ICANN org has updated the Issue Report accordingly and included a summary of the comments (see Annex C), which is now submitted as the Final Issue Report to the GNSO Council for its consideration.

2 Procedural Foundation

2.1. Grounds for submission

This Final Issue Report is submitted in accordance with Step 2 of the Policy Development Process described in Annex A of the ICANN Bylaws.[1]

2.2. The identity of the party submitting the request

The GNSO Council.

2.3. Support for the issue to initiate a PDP

On 24 June 2020, the GNSO Council passed a motion, requesting ICANN org to draft a Preliminary Issue Report on the issues identified in the Transfer Policy Review Initial Scoping Paper, which was requested as part of the GNSO Council's review of the Transfer Policy.

2.4. How that party is affected by the issue

The Transfer Policy has a direct impact on the business operations of Registrars and Registries and provides Registrants (both individuals and organizations) with the ability to safely transfer their domain names from one registrar to another. Therefore, the Transfer Policy affects many, if not all, of the GNSO's Stakeholder Groups (SGs) and Constituencies (Cs). Recommendations that may be developed as a result of a GNSO PDP on the Transfer Policy may also be of interest to other ICANN Supporting Organizations (SOs) and Advisory Committees (ACs) because the Transfer Policy allows for increased consumer choice and competition. Additionally, the Transfer Policy is aimed at preventing fraudulent domain name transfers and domain name hijacking.

2.5. Issue under consideration

Further to the Transfer Policy Review Scoping Team's recommendation to the GNSO Council to instruct ICANN org to draft a Preliminary Issue Report, outlining, et.al., the issues described within the Transfer Policy Initial Scoping Paper, the GNSO Council will now review the issues contained in this Report and determine if it should launch a PDP.

2.6. Legal scope to launch Policy Development Process

Based on the documentation above, the launch of a dedicated policy development process (PDP) to consider, at a minimum, the issues identified in this Final Issue Report has been confirmed by ICANN's

[1] See: http://www.icann.org/general/bylaws.htm#AnnexA.

General Counsel to be properly within the scope of the GNSO and the ICANN Policy Development Process.

2.7. Publication of Preliminary Issue Report

In accordance with the GNSO Policy Development Process, the ICANN org published a Preliminary Issue Report for public comment in order to allow for community input on additional information that may be missing from the Preliminary Issue Report, or the correction or updating of any information in the Preliminary Issue Report. In addition, the public comment period allowed for members of the ICANN Community to express their views to the GNSO Council on whether or not to initiate a PDP. Following review of the public comments received, ICANN org has updated the Issue Report accordingly and included a summary of the comments (see Annex C), which is now submitted as the Final Issue Report to the GNSO Council for its consideration.

3 Discussion of Issues

3.1. Overview of Issues

This Section provides an overview of all relevant issues related to the GNSO Council request for this Final Issue Report as summarized in the Transfer Policy Review Scoping Paper.[2] In addition, it provides references to relevant documentation, ongoing and completed work efforts, and other applicable information.

3.1.1. Gaining & Losing Registrar Form of Authorization ("FOA")

3.1.1.1. Overview of a Standard Inter-registrar Transfer (pre-GDPR)

Before the ICANN Board's adoption of the Temporary Specification for gTLD Registration Data and subsequent adoption of the Interim Registration Data Policy for gTLDs, the standard inter-registrar transfer consisted of the following seven steps:

(1) The Registered Name Holder contacts the registrar it would like to transfer its domain name to, also referred to as the Gaining Registrar.
(2) Assuming the domain name is eligible for inter-registrar transfer,[3] the Gaining Registrar will require the Registered Name Holder[4] to confirm their intent to transfer the domain name by sending the Registered Name Holder a Form of Authorization ("FOA"), also referred to as the Gaining Registrar FOA or Gaining FOA.
(3) The Registered Name Holder must "acknowledge" the FOA, i.e., confirm they would like to transfer the domain name to the Gaining Registrar. Generally speaking, acknowledging the FOA means clicking a designated link in an email sent from the gaining registrar to the registered name holder.
(4) Upon receipt of the FOA, the Gaining Registrar notifies the relevant Registry Operator of the inter-registrar transfer.[5]
(5) The Registry Operator sends a notice of the pending transfer request to the Gaining Registrar and to the registrar of record, or "Losing Registrar".

[2] Pages 3-7 of the Transfer Policy Review Scoping Team's paper includes a table of the issues identified by the Transfer Policy Scoping Team.
[3] The gaining registrar will confirm the domain name is "unlocked" and the registered name holder has provided an "AuthInfo" code.
[4] Specifically, the gaining registrar is required to send the FOA to the "transfer contact," which is defined as the registered name holder or the "Administrative Contact," as listed in the losing registrar's or applicable registry's (where available) publicly accessible RDDS service. In the event of a dispute, the registered name holder's authority supersedes that of the Administrative Contact.
[5] The gaining registrar will also submit the AuthInfo code to the registry operator.

(6) The Losing Registrar must send the Registered Name Holder a notice of the pending transfer to confirm the Registered Name Holder's intent to transfer the domain name. This notice is also referred to as the Losing Registrar FOA or Losing FOA. In certain enumerated circumstances, the Losing Registrar must deny the transfer request, e.g., the domain is the subject of a court order or UDRP proceeding and cannot be transferred.[6]
(7) If after five calendar days, the Registry Operator has not received any objection to the inter-registrar transfer, it will process the transfer request.[7]

3.1.1.2. Overview of the standard inter-registrar process post-GDPR

Following the ICANN Board's adoption of the Temporary Specification for gTLD Registration Data on 17 May 2018, the Transfer Policy requirements were partially amended to account for situations where the Gaining Registrar is unable to send the Gaining FOA due to its inability to obtain current registration data via the public Registration Data Directory Services ("RDDS"). This is because the Registrar of Record (or Losing Registrar) may be required to redact certain registration data due to data protection law requirements.

The Temporary Specification for gTLD Registration Data provides, in Appendix G, where a gaining registrar is unable to obtain current registration data via RDDS, the following steps apply:

(1) The Registered Name Holder contacts the registrar it would like to transfer its domain name to, also referred to as the Gaining Registrar.
(2) Assuming the domain name is eligible for inter-registrar transfer, the Registered Name Holder must independently re-enter registration data with the Gaining Registrar. (emphasis added to highlight update)
(3) The Gaining Registrar notifies the relevant Registry Operator of the inter-registrar transfer.
(4) The Registry Operator must verify the request is valid—i.e., confirm that the AuthInfo code provided by the Gaining Registrar is legitimate—in order to accept an inter-registrar transfer request. (emphasis added to highlight update)
(5) The Registry Operator sends a notice of the pending transfer request to the Gaining Registrar and to the registrar of record, also referred to as the Losing Registrar.
(6) The Losing Registrar must send the Registered Name Holder a notice of the pending transfer to confirm the Registered Name Holder's intent to transfer the domain name (the Losing FOA). In certain enumerated circumstances, the Losing Registrar must deny the transfer request (e.g., the domain is the subject of a court order and cannot be transferred).
(7) If after five calendar days, the Registry Operator has not received any objection to the inter-registrar transfer, it will process the transfer request.

[6] The Losing Registrar is required to send the standard Form of Authorization for losing registrars.

[7] It is worth noting that the transfer may proceed before the close of five calendar days. For example, the Losing Registrar may include the ability to approve the inter-registrar transfer request within its Losing FOA, and if the registrant acknowledges the Losing FOA, the transfer could proceed before the close of five business days.

In short, the Losing Registrar, or Registrar of Record, is still required to send the Losing FOA to the registered name holder, but the Gaining Registrar is not required to send the Gaining FOA if it is unable to obtain the registered name holder's current registration data via RDDS.

In its review of the Temporary Specification, the EPDP Team recommended[8] the above-described workaround provided in the Temporary Specification, whereby the gaining registrar is not required to send the Gaining FOA if it is unable to obtain the registered name holder's current registration data via RDDS, be maintained until the Transfer Policy has been reviewed by the GNSO Council.

On 15 May 2019, the ICANN Board adopted the GNSO Council Recommendations for a new Consensus Policy on gTLD Registration Data, as set forth in Section 5 of the Final Report of the GNSO's Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data in accordance with its accompanying scorecard.

On 31 October 2019, the GNSO Council wrote to the Board, noting that ICANN org's interpretation of the language in the Interim Registration Data Policy for gTLDs had resulted in an untenable situation for registrars. Specifically, the Registrar Stakeholder Group notes the problematic interpretation with ICANN org's position that a Gaining Registrar is required to send a Form of Authorization ("Gaining FOA") where the email address "is available". The letter provides "even where the registrant email field exists in the WHOIS output, the email does not go directly to the registrant due to the use of web forms or pseudonymized email addresses. If a registrar implemented such a system, there is no guarantee that the email will reach the registrant. In short, registrars are unable to build a reliable automated process to continue processing the large volume of transfers between registrars, which will, in turn, defeat the purpose of the Transfer Policy." At that time, the GNSO Council specifically noted the need for the Gaining FOA and the corresponding language in the Temp Spec to be further discussed as a matter for future policy development.

Following the receipt of this letter, the ICANN Board passed a resolution to defer contractual compliance enforcement of the gaining registrar's requirement to obtain express authorization of an inter-registrar transfer from the Transfer Contact via the Standardized Form of Authorization (FOA). Accordingly, ICANN Contractual Compliance is deferring enforcement of Section I(A)(2.1) of the Transfer Policy until the matter is settled in the GNSO Council's Transfer Policy review. For reference, Section I(A)(2.1) of the Transfer Policy provides: "[o]btain express authorization from either the Registered Name Holder or the Administrative Contact (hereafter, 'Transfer Contact'). Hence, a transfer may only proceed if confirmation of the transfer is received by the Gaining Registrar from the Transfer Contact." The sections following I(A)(2.1) provide details on how the previously-required express authorization was expected to occur.

3.1.1.3. Previous Policy Work on the FOA

The issue of both the necessity and utility of FOAs has been the subject of previous policy development and is a continued source of discussion within the ICANN community.

In its deliberations, the GNSO IRTP Part C Working Group observed that the use of EPP Authorization Info (AuthInfo) codes has become the de facto mechanism for securing domain transfers, and the

[8] Please refer to Recommendation 24 of the EPDP Team's Phase 1 Final Report.

AuthInfo code had obviated the reason for the creation of the standard FOA. As a result, the WG recommended that the GNSO Council consider adding this issue to the IRTP Part D.

In the GNSO IRTP Part D PDP Working Group, the GNSO chartered the Working Group to review the following question: "Are FOAs still necessary? h) Whether the universal adoption and implementation of EPP AuthInfo codes has eliminated the need of Forms of Authorization (FOA)s."

In reviewing this issue, the IRTP Part D PDP Working Group ultimately recommended maintaining the FOA. Specifically, recommendation 17 provides: "[t]he WG does not recommend the elimination of FOAs. However, in light of the problems regarding FOAs, such as bulk transfers and mergers of registrars and/or resellers, the Group recommends that the operability of the FOAs should not be limited to email. Improvements could include: transmission of FOAs via SMS or authorization through interactive websites. Any such innovations must, however, have auditing capabilities, as this remains one of the key functions of the FOA."

In its deliberations on this topic, some members of the Working Group believed the FOA was no longer necessary and was ultimately causing unintended harm by complicating legitimate inter-registrar transfer requests. These Working Group members believed that the discontinuation of FOAs would reduce the rate of abandonment of legitimate transfer attempts. These WG members also observed that FOAs do not uniquely identify Registered Name Holders. In other words, they believed the FOA resulted in a double authorization, which was unnecessary in light of the AuthInfo code requirement.

Other Working Group members noted that the FOA was useful in a number of circumstances, including, for example, its role as a "paper trail" that could be used in the auditing of inter-registrar transfers issues and disputes. The Working Group additionally noted the FOA may be a useful tool for gTLD registries, as gTLD registries do not have a contractual or business relationship with the registered name holder.

The Working Group observed the FOA is likely a factor contributing to registered name holder's confusion with inter-registrar transfers; however, it noted that, at the time of its deliberations, it did not have sufficient data to recommend the outright elimination of the FOA. The Working Group also noted, at the time of publishing its Final Report, many of the IRTP recommendations from Working Groups Part B and C had not yet been implemented; accordingly, the Working Group felt it would be premature to eliminate the FOA before the impact of the updated Transfer Policy could be considered. The Working Group did, however, stress that a future review of the Transfer Policy should consider the need for FOAs, and, to that end, it requested ICANN org begin gathering related Transfer Policy metrics.

3.1.1.4. Input Received in Response to the Policy Status Report

In its preparation of the Transfer Policy Status Report, ICANN org created an online survey to gather input on many general and specific aspects of the IRTP. The survey included 29 questions, and the results of the survey can be viewed here: https://www.surveymonkey.com/results/SM-Q2J8JZRQV/. The questions and responses specifically related to the utility and security of FOAs are provided below for reference.

In response to the question, "On a scale of 1 to 10, how effective is the transfer policy generally as it exists today (10 being most effective)?" the overall response was 6/10.[9] In its comment on this question, the Registrar Stakeholder Group, who believed the process was a "6 or 7," noted the FOA and other processes are unnecessary and do not prevent hijacking or fraudulent transfers.

Other respondents noted:

- Form of Authorization and email authorization not secure means to validate transfers.
- Removing the requirement of an FOA to WHOIS has helped immensely.

Question 1 of the survey provided "[i]n your view, did the Form of Authorization (FOA) requirement work to mitigate problems surrounding unauthorized domain transfers? How might this requirement be improved or changed to mitigate such problems?" In response, most respondents indicated that the FOA was no longer required, was an annoyance or complication for customers, and is now outdated. Respondents also noted that the use of email to send/receive the FOA was problematic given that many hijacking cases are a result of a registrant's email already having been compromised. Respondents indicated that AuthInfo Codes within EPP and domain locking at the losing registrar provide sufficient security.

One respondent's answer was generally representative of the negative responses:

"The FOA was helpful to compare contact details for the gaining and losing registrar, but every time the details were the same surrounding unauthorized transfers; meaning the hijacking always happened before the transfer request itself."

Another replied:

"We saw no increase in issues since the FOA has not been required under [the] Temp Spec and therefore feel it does not add any value."

A small number of respondents replied that the FOA was useful in that it created a paper trail for transfer issues and ensured that a registrant understood his/her domain was being transferred.

The RrSG noted that responses varied within their group:

"Some registrars find that the FOA increases risk because it relies on a non-secure method (email), which can be accessed improperly to transfer a domain without the [registered name holder's] approval. Other registrars find that the FOA helps mitigate problems by ensuring the current registrant understood the domain was transferring to a new registrar. There is agreement that we should move away from the FOA and focus on [AuthInfo Code] security."

In response to Question 10, which provided: "Do you think the FOA should continue to be a requirement given most systems are now based on the Extensible Provisioning Protocol (EPP)? Why or why not?," respondents noted:

[9] For each "Answer Breakdown" table in this report, the "Weighted Average" reflects the average star rating given by respondents (no special weights were assigned to any response field). This is rounded to the nearest whole number in the results presented in "Overall" field directly above each table.

- "FOA approval should continue. Some Registrants might inadvertently share their EPP code without understanding the effects. Approval from the Registrant email is a must."
- "…FOA should absolutely remain. Even if it never comes up in 99.9% of cases those additional records can help resolve potential issues or disputes when they arise and have proven invaluable in the past."
- "…all efforts to confirm a transfer should be taken to protect the owners."
- "…still [need] the FOA process…Without FOA, as a registrar, we are unable to provide this to [a] judge."
- "Having the FOA included as part of the transfer process lets us pull additional information should there ever be a dispute or claim of hijacking with a domain transfer and ensure it is handled correctly. It's always better to have more records and be over-prepared than not."

The negative responses argued that technical solutions are available which obviate the need for the FOA. These responses include:

- "No, because all you need is the [AuthInfo Code]. The FOA only adds 'paperwork' to the process and does not provide any protection."
- "No, there are technical ways to ensure that the transfer was requested by the registrant that do not require additional emails be sent."
- "No, FOA is redundant to people who have confirmed that they want to transfer. And unable to suppress unauthorized domain transfers."

Some negative responses offered solutions to maintain domain transfer security without the FOA:

- "No, because the password itself should be enough (plus domain transfer lock)…however…there should be work around a scheduled EPP password rotation or expiration…"
- "Due to GDPR the FOA process is broken and we need to get rid of it. Short lived Transfer Tokens in the EPP could be a solution."
- "Most systems are already based on EPP. With the Temp Spec we can no longer do FOA. Therefore we should have better security surrounding [AuthInfo Codes]."

The RrSG provided a detailed response:

"No. Prior to Temp Spec changes, the FOA functioned as a second factor of authentication for the transfer, but was cumbersome for the Registered Name Holder to use effectively. Removing the FOA requires the enhancement of other security measures, specifically the [AuthInfo Code]. There should be best-practice guidelines for [AuthCode] security; TechOps leans towards Registrars bearing the responsibility for the [AuthCode]."

In response to Question 11, which provided: "It is no longer required for the losing registrar to provide the FOA as a result of the "Temporary Specification for gTLD Registration Data." Is this a transfer solution you support? Do you have concerns with this? Please explain your answer," respondents tended to answer in the affirmative.

In general, respondents noted that they experienced few or no issues when the requirement was removed as a result of the GDPR/Temp Spec, and that redacting much of the public WHOIS increased security in-and-of itself.

For example, some respondents replied with the following:

- "We support the elimination of the FOA…that is, we support simply making the 'Temporary Specification for gTLD Registration Data' permanent…In fact, the lack of public WHOIS data is almost certainly making domain names more secure against hijacking, as it prevents malicious actors from using WHOIS to determine which email address they need to compromise to hijack a domain name."
- "Yes, this is how the thefts are occurring. It is too easy to create a new fake account and request the transfer."
- "The GDPR is now in effect for more than 175 days. If there were issues they would have emerged already. But we have observed no issues and is in line with our experience as a ccTLD registrar for many large ccTLDS which have no FOA requirement."[10]
- "Yes we support the [removal of the FOA requirement]. Transfers should be redesigned to a) [be] GDPR compliant b) real time and c) safer."

As in previous questions on the FOA, some respondents suggested relying on the AuthInfo code as a default method to verify transfers and increasing security of those codes. This is discussed further in the next section of this Report.

Lastly, survey respondents were also asked which methods are used to mitigate domain name hijacking outside of the Transfer Policy framework?

Survey respondents noted the following:

- Direct verification—either via phone call, email, or paper form—from clients prior to taking action on a domain
- Domains only placed in unlock status once registrant confirms transfer via direct verification
- Two-factor authentication
- Manual comparison of IP addresses and other available customer data with customer's historical IP addresses and data
- Regular updates to and high security standards for transfer AuthCodes, one respondent noted

3.1.1.5. TechOps Proposal

During its consideration of the Gaining Registrar FOA issue, the Transfer Policy Review Scoping Team noted that future consideration of the Transfer Policy should review the proposed transfer process from Contracted Party House Tech Ops Subcommittee ("CPH TechOps Group"). For background, the CPH TechOps Group was founded by ICANN's Registrars Stakeholder Group and Registries Stakeholder Group in September 2017 in an effort to discuss and address the technical and operational needs of ICANN-accredited registrars and registries.

In May 2018, the CPH TechOps group convened two workshops at ICANN's Generic Domains Division ("GDD") Summit, during which the group explored how the Transfer Policy could properly function once GDPR went into effect. The group was unable to come to a final agreement on an updated transfer

[10] Note - while the overall number of Transfer Policy-related complaints has decreased, there is no data confirming the cause of the decrease.

process during the Summit; however, the members in attendance agreed on a set of high-level principles, which are included below for reference:

- The transfer process must comply with current data privacy regulations
- The transfer process must be instant, however a time to validate the legitimacy of transfer should be given
- A transfer token shall be sufficient to authorize a transfer
- No personal data shall be transferred from the old (losing) to the new (gaining) Registrar
- The existing gTLD Transfer Policy should be changed as little as possible

In its review of the inter-registrar transfer process for gTLD names, the CPH TechOps group observed the proposed updated process could be divided into three distinct phases, namely:

- Phase 1: The registrant initiates the transfer process with its current registrar (the losing registrar)
- Phase 2: The registrant requests an inter-registrar transfer to the registrar to whom it would like to sponsor its name (the gaining registrar)
- Phase 3: The registry operator effects the transfer from the losing registrar to the gaining registrar

Using these three phases, the CPH TechOps Group delineated the proposed, updated required steps, proposed policy updates, and associated technical requirements. The detailed CPH TechOps Proposal can be found in Annex B.

3.1.1.6. Further Policy Questions for Consideration

Gaining FOA

1. 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?
2. 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)?
3. 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?

4. 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.?
5. 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?

Additional Security Measures

6. 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?

Losing FOA

7. Is the Losing FOA still required? If yes, are any updates necessary?
8. 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?
9. 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?

3.1.2. AuthInfo Code Management

3.1.2.1. Overview of the AuthInfo Code

The AuthInfo Code, also referred to as the Auth-Code, the Authorization Code, the transfer key, or the transfer code, is a unique code created by a registrar to identify the registrant of the domain name. Registrars must administer the unique AuthInfo Code on a per-domain name basis, and the AuthInfo Code is required for the registrant to transfer its domain name from one registrar to another. As described in Section 3.1.1.1 above, in order for an inter-registrar transfer to proceed, the Gaining Registrar must confirm a domain name is eligible for an inter-registrar transfer, which requires it to (1) confirm the domain name is unlocked, and (2) the registrant has provided the AuthInfo Code.

The Losing Registrar will generally provide the AuthInfo Code to a registrant in one of two ways:

1. Via the control panel, which is the section of the registrant's domain name account under which it can modify the domain name settings such as nameservers or contact information; OR
2. In response to a request from the registrant, the registrar is required, under the Transfer Policy, to provide the AuthInfo Code to the registrant within five calendar days of receiving the registrant's request. The AuthInfo Code could be provided by email or SMS message, for example.

Section I.A.5 of Transfer Policy details the requirements related to the AuthInfo Code. Specifically:

1. Registrars must provide the Registered Name Holder with the unique "AuthInfo" code within five (5) calendar days of the Registered Name Holder's initial request if the Registrar does not provide facilities for the Registered Name Holder to generate and manage their own unique AuthInfo Code (Section I.A.5.2)
2. Registrars must not employ any mechanism for complying with a Registered Name Holder's request to obtain the applicable AuthInfo Code that is more restrictive than the mechanisms used for changing any aspect of the Registered Name Holder's contact or name server information (Section I.A.5.3)
3. Registrars must not refuse to release an AuthInfo Code to the Registered Name Holder solely because there is a dispute between the Registered Name Holder and the Registrar over payment (Section I.A.5.4)
4. AuthInfo codes must be unique and on a per-domain basis (Section I.A.5.5)
5. AuthInfo codes must be used solely to identify a Registered Name Holder (Section I.A.5.6)

3.1.2.2. Previous Policy Work on AuthInfo Codes

GNSO Council Transfer Policy Task Force

The GNSO Council Transfer Policy Task Force, which completed its work in 2003, examined the current state of domain portability, or, the ability of registrants to transfer their domain names from one registrar to another. Following consultation with interested and impacted members of the community, the Task Force ultimately determined that registrants could not easily transfer their domain names to another registrar. Accordingly, the Transfer Policy Task Force submitted 29 consensus policy recommendations for the Name Council's consideration. The three recommendations pertaining to AuthInfo Codes are included below for ease of reference:

Recommendation 6: In EPP-based gTLD Registries,[11] Registrars must provide the Registrant with the Registrant's unique "AuthInfo Code" within a reasonable period of time of the Registrant's initial request. The Task Force observes support that this reasonable time period is 72 hours or a similarly limited period of time.

Recommendation 7: In EPP-based gTLD Registries, Registrars may not employ any mechanism for a Registrant to obtain its AuthInfo Code that is more restrictive than what they require from a Registrant to change any aspect of its contact or nameserver information.

[11] EPP stands for Extensible Provisioning Protocol and is a protocol used as an authenticated and secure channel of communication between the Registry and Registrar, which can also be used in the context of transfers.

Recommendation 15: In EPP-based TLDs, a Losing Registrar must not refuse to release an [AuthInfo Code] to the Registrant solely because there [is] a dispute between a Registrant and the Registrar over payment.

These requirements, or slight variations thereof, currently appear in the Transfer Policy in Section I.5.2, I.5.3, and I.5.4, respectively.

GNSO IRTP Part D PDP Working Group

As noted in Section 3.1.1.3 of this report, the GNSO IRTP Part D PDP Working Group, which completed its work in 2014, examined the question of whether the universal adoption and implementation of EPP AuthInfo Codes has eliminated the need for FOAs. The Working Group ultimately came to the conclusion that it was not appropriate to remove the FOA policy requirement at that time but did recommend ICANN gather metrics for future policy work on this issue.

Since the work of the GNSO IRTP Part D PDP Working Group, there has not been further GNSO work on AuthInfo Codes specifically. The CPH Tech Ops Group has flagged some questions for future policy development work, and these questions are outlined in Section 3.1.2.5 of this Report.

3.1.2.3. Input Received in Response to the Policy Status Report

As described in Section 3.1.1.4, ICANN org created an online survey to gather input on many general and specific aspects of the IRTP, as part of its creation of the Transfer Policy Status Report.

Some survey respondents referenced AuthInfo Codes, and these responses have been included below for reference.

Question 7: What methods do you use to mitigate domain name hijacking outside of the IRTP framework?

Survey respondents noted the following:

- Direct verification—either via phone call, email, or paper form—from clients prior to taking action on a domain
- Domains only placed in unlock status once registrant confirms transfer via direct verification
- Two-factor authentication
- Manual comparison of IP addresses and other available customer data with customer's historical IP addresses and data
- Regular updates to and high security standards for transfer AuthCodes, one respondent noted

Question 10: Do you think the FOA should continue to be a requirement given most systems are now based on the Extensible Provisioning Protocol (EPP)? Why or why not?

The RrSG noted, in part, "[r]emoving the FOA requires the enhancement of other security measures, specifically the [AuthInfo Code]. There should be best-practice guidelines for [AuthInfo Code] security; TechOps leans towards Registrars bearing the responsibility for the [AuthInfo Code]."

Question 11: It is no longer required for the gaining registrar to provide the FOA as a result of the "Temporary Specification for gTLD Registration Data." Is this a transfer solution you support? Do you have concerns with this? Please explain your answer. In response, some survey respondents noted:

"We strongly suggest changes in registry-level auth-info practices for domain security."

"I am concerned about who receive[s] [the AuthCode][.] [I]f we could confirm that only [the] registrant can receive [the AuthCode], then we may no longer need FOA."

Question 19: In general, what issues are your customers having, if any, as they relate to transfers?

The RrSG noted the following: [It's] [d]ifficult for Registered Name Holders to retrieve [AuthInfo Codes] for a long list of domains as there are no requirements to permit bulk [AuthCode] requests.

Question 28: In your view, what could be improved in regard to making domain name transfers?

A registrant responded with the following: "While the [AuthInfo Code] is a good system, I should also be able to transfer my domain name without any intervention from the outgoing registrar, should that one not be cooperative."

3.1.2.4. CPH Tech Ops AuthInfo Code Research

During ICANN63 in Barcelona, the CPH Tech Ops Group reviewed various topics in relation to its proposed updated transfer process.[12] Two of the topics related specifically to AuthInfo Codes and have been provided below for reference.

[12] New gTLD Transfer Process CPH Discussion Paper v.01

The CPH Tech Ops Group first discussed which entity (registrar or registrar) should be responsible for AuthInfo Codes and the corresponding TTL.[13] The Group noted the registry should be responsible for the storage and processing of the AuthInfo Code in order to "to reach a uniform, transparent, and predictable process". The Group also recommended that before the new requirements for registries went into effect, a to-be-developed best practices guide around AuthInfo Codes should be provided to registrars.

The CPH Tech Ops Group also discussed possible values and syntax requirements for the AuthInfo Code. The Group ultimately recommended the AuthInfo Code TTL should be no more than 14 days. The Group also concluded that there should be further policy work on the syntax requirements for the AuthInfo Code. For further reading on the CPH Tech Ops Group, please refer to Annex B of this report.

3.1.2.5. Further Policy Question for Consideration

Auth-Info Codes Details

1. Is AuthInfo Code still a secure method for inter-registrar transfers? What evidence was used by the Working Group to make this determination?
2. 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?
3. 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?
4. 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.)?

Bulk Use of Auth-Info Codes

5. Should the ability for registrants to request AuthInfo Codes in bulk be streamlined and codified? If so, should additional security measures be considered?
6. Does the CPH TechOps research provide a logical starting point for future policy work on AuthInfo Codes, or should other options be considered? 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?

[13] TTL stands for "Time to Live," and is a mechanism that limits the lifespan or lifetime of data in a computer or network.

3.1.3. Change of Registrant ("CoR") or Inter-Registrant Transfers

3.1.3.1. Overview of theChange of Registrant Process and Requirements

Change of Registrant (CoR) requirements seek to ensure that certain changes to registrant information have been authorized by requiring registrars to obtain confirmation from the Prior Registrant[14] and New Registrant[15] before these changes are made. Specifically, CoR policy requirements are applicable under the Transfer Policy when a material change[16] is made to one or more of the following: the Prior Registrant name, Prior Registrant organization, Prior Registrant email address, and/or Administrative Contact email address, if there is no Prior Registrant email address (Section II.A.1.1). In practice, this means that CoR provisions apply when a domain is transferred from one registrant to another registrant, as well as when there is no inter-registrant transfer but the registrant updates certain registration information.

A key component of the CoR process is the "60-day inter-registrar transfer lock," which prevents transfer to another registrar for sixty (60) days following an update that qualifies as a CoR. According to the IRTP Part C Working Group's recommendations, which served as a basis for the CoR policy requirements, "The 60-day lock is used to 'contain' the changes of Registrants within a single Registrar in order to facilitate recovery of domains that have been hijacked" (Note G to Recommendation 1). Put another way, the CoR lock is intended to prevent hackers from fraudulently changing contact information in a registration data directory service in order to transfer a domain for malicious purposes. Regarding implementation of the 60-day lock:

- The registrar may give the Prior Registrant the option to opt out of the 60-day lock prior to a Change of Registrant request (Section II.C.2).
- 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 (see footnote 4 to section II.C.1.2).

To complete the CoR process, Registrars must complete the following steps, summarized at a high level:

1. Confirm the domain name is eligible for Change of Registrant (Section II.C.1.1).[17]
2. Obtain confirmation of the Change of Registrant request from the New Registrant, or a Designated Agent of the New Registrant, and provide certain required notifications (Section II.C.1.2).[18]

[14] According to Section II.A.1.4 of the Transfer Policy, "Prior Registrant" means the Registered Name Holder at the time a Change of Registrant is initiated.

[15] According to Section 11.A.1.5 of the Transfer Policy, "New Registrant" means the entity or person to whom the Prior Registrant proposes to transfer its domain name registration.

[16] Section II.A.1.3 of the Transfer Policy defines Material Change to mean a non-typographical correction. Additional guidance in this regard is provided in the notes to the Transfer Policy.

[17] According to Transfer Policy Section II.B.1, "In general, registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely." However, Section II.B.2 describes specific circumstances under which a Registrar must deny Change of Registrant.

[18] The Designated Agent is defined as an individual or entity that the Prior Registrant or New Registrant explicitly authorizes to approve a Change of Registrant on its behalf (Section II.A.1.2).

3. Inform the Prior Registrant or its Designated Agent that if its final goal is to transfer the domain name to a different registrar, the Prior Registrant is advised to request the inter-registrar transfer before the Change of Registrant to avoid triggering the 60-day lock (Section II.C.1.3).
4. Obtain confirmation of the Change of Registrant request from the Prior Registrant, or the Designated Agent of the Prior Registrant (Section II.C.1.4).
5. Process the Change of Registrant within one (1) day of obtaining the confirmations (Section II.C.1.5).
6. Notify the Prior Registrant and New Registrant before or within one day of the completion of the Change of Registrant (Section II.C.1.6). This notification includes informing the Prior Registrant and New Registrant of the 60-day inter-registrar transfer lock or informing the Prior Registrant that it previously opted out of the 60-day inter-registrar transfer lock (Section II.C.1.6.4).
7. Impose a 60-day inter-registrar transfer lock, unless the Registered Name Holder had previously opted out (Section II.C.2).

3.1.3.2. Previous Policy Work Regarding Change of Registrant

The Final Report of the IRTP Part B Working Group, which completed its work in 2011, included a recommendation that an Issue Report should be requested on the topic of "change of control," which it defined as "moving the domain name to a new Registered Name Holder."[19] In requesting the Issue Report for the third PDP in the IRTP series, the GNSO Council included "change of control" in the list of items to be considered, in line with the recommendation from the IRTP Part B Working Group.

The IRTP Part C Working Group, which completed its work in 2012, was subsequently launched and chartered to address three questions, including the following, as outlined in the Final Issue Report:

- "Change of Control" function, including an investigation of how this function is currently achieved, if there are any applicable models in the country-code name space that can be used as a best practice for the gTLD space, and any associated security concerns. It should also include a review of locking procedures, as described in Reasons for Denial #8 and #9, with an aim to balance legitimate transfer activity and security.

The Working Group's deliberations were structured around a series of questions included in the Working Group's charter and are summarized in the Working Group's Final Report.

[19] The IRTP Part-B Working Group's Recommendation 4 states: "The WG notes that the primary function of IRTP is to permit Registered Name Holders to move registrations to the Registrar of their choice, with all contact information intact. The WG also notes that IRTP is widely used to affect a "change of control," moving the domain name to a new Registered Name Holder. The IRTP Part B WG recommends requesting an Issue Report to examine this issue, including an investigation of how this function is currently achieved, if there are any applicable models in the country-code name space that can be used as a best practice for the gTLD space, and any associated security concerns. The policy recommendations should include a review of locking procedures, as described in Reasons for Denial #8 and #9, with an aim to balance legitimate transfer activity and security. Recommendations should be made based on the data needs identified in the IRTP Part B workgroup discussions and should be brought to the community for public comment. The WG would like to strongly encourage the GNSO Council to include these issues (change of control and 60-day post-transfer lock) as part of the next IRTP PDP and ask the new working group to find ways to quantify their recommendations with data."

In considering how “change of control” or “change of registrant” functions were achieved at the time, the Working Group found that a process was implied, for example, in the Uniform Dispute Resolution Policy, but that it was handled in different ways by registrars in practice. The Working Group recognized that having minimum requirements could clarify and simplify the process while reducing problems that had been encountered when using the IRTP to enact a change of control.

The Working Group considered whether there were any applicable models in the country-code name space, drawing on input from the ccNSO and different registrars who also manage ccTLD registrations. In its analysis, the Working Group found that there was significant variation in the way Change of Registrant is implemented by ccTLDs.

In its deliberations, the Working Group reviewed existing locking procedures, as described in Reasons for Denial #8 and #9:

- Reason for Denial #8: The transfer was requested within 60 days of the creation date as shown in the registry Whois record for the domain name.
- Reason for Denial #9: A domain name is within 60 days (or a lesser period to be determined) after being transferred (apart from being transferred back to the original Registrar in cases where both Registrars so agree and/or where a decision in the dispute resolution process so directs). "Transferred" shall only mean that an inter-registrar transfer has occurred in accordance with the procedures of this policy.

The Working Group concluded that Reason for Denial #9 should also apply to a change of registrant, i.e. following a change of registrant, it should not be possible to initiate a change of registrar for a 60-day time period. This conclusion led to a recommendation to codify the 60-day lock in policy.

In October 2012, The IRTP Part-C Working Group published its Final Report which included a recommendation regarding change of registrant, excerpted here for ease of reference:

> *Recommendation #1 – The IRTP Part C WG recommends the adoption of change of registrant consensus policy, which outlines the rules and requirements for a change of registrant of a domain name registration. Such a policy should follow the requirements and steps as outlined hereunder in the section ‘proposed change of registrant process for gTLDs’. . .*
>
> *STEP 0: If the Prior and New Registrants are transferring the domain to a new registrar in conjunction with this Change of Registrant process, it is suggested that they first complete the Inter-Registrar Transfer in order to avoid triggering the default 60- day lock associated with the Change of Registrant process. Note that the Inter Registrar Transfer policy is revised so as to not permit changes to Registrant information at the same time as an inter-registrar transfer. The Gaining Registrar must validate this prior to completing the transfer. . .*
>
> *STEP 1: Both Registrants authorize the change*
>
> - *Either the Prior or Gaining Registrant produces and transmits Change of Registrant Credentials to the other Registrant*
> - *The other Registrant acknowledges the receipt of credentials and authorizes the transfer*

STEP 2: Registrar determines that both Prior and New Registrant have authorized the Change of Registrant and that the domain is eligible for Change of Registrant (i.e. there are no locks or other restrictions on the domain)

STEP 3: Registrar changes registrant

STEP 4: Registrar notifies Prior and New Registrant of the change that has taken place

STEP 5: Registrar places a lock on the domain to prevent Inter-Registrar transfers of the domain for 60 days, unless the Prior Registrant has opted out of this requirement after having received a standard notice as to the associated risks. . .[20]

In the Final Report, the Working Group noted the following with respect to the expected impact of the recommended process: "The WG expects that adopting the proposed process for a change of registrant as outlined in the section 'proposed change of control process for gTLDs' will usefully clarify and standardize how a change of registrant can be conducted and as a result help reduce issues encountered when the IRTP is used to enact a change of registrant as well as reduce registrant confusion over how to complete a change of registrant."

As recommended by the IRTP Part C Working Group in Note I to Recommendation 1, the IRTP became a hybrid Transfer Policy with two parts: one detailing the policy for a change of registrar, and another detailing the policy for a change of registrant. The steps described in Recommendation 1 of the IRTP Part C Working Group's Final Report served as a basis for developing Part II of the hybrid Transfer Policy, which had a policy effective date of 1 December 2016.

3.1.3.4. Change of Registrant for Registrations Using Privacy/Proxy Services

On 1 December 2016, the day that IRTP Part C recommendations went into effect, the GNSO Council sent a letter to the ICANN Board sharing concerns raised by the Registrar Stakeholder Group regarding implementation of Change of Registrant for registrations that use privacy and proxy services. The policy recommendations were silent with respect to the addition and removal of privacy/proxy services. The planned implementation interpreted the policy to require registrars to implement the Change of Registrant, and therefore the 60-day inter-registrar transfer lock, when any change is made to the public Whois data, regardless of whether that change results in a change to the underlying customer data. The GNSO presented a series of use cases demonstrating potential harms associated with this interpretation. It asked the Board to instruct ICANN org to defer compliance enforcement on the removal or addition of privacy/proxy within the Transfer Policy and work with the Registrar Stakeholder Group and other interested parties to evaluate alternatives to address the implementation concerns.

The ICANN Board responded to the GNSO Council on 21 December 2016, stating that it had instructed the ICANN President and CEO to defer compliance enforcement on the removal or addition of privacy/proxy within the Transfer Policy until implementation issues have been resolved. The ICANN Board confirmed these instructions in a resolution adopted on 3 February 2017.

The Registrar Stakeholder Group discussed this issue further, consulted with other interested parties, and recommended that the issue be further evaluated by the Privacy & Proxy Services Accreditation

[20] For full text of the recommendation, please see the Final Report.

Issues Implementation Review Team (PPSAI IRT). On 30 November 2017, The GNSO Council adopted a resolution directing the PPSAI IRT to consider the issue of privacy/proxy registrations and IRTP Part C.

ICANN org's implementation of PPSAI slowed with the launch of the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data (EPDP), because the same issues that need to be resolved to finalize PPSAI implementation were under active discussion in the EPDP. On 4 March 2019, ICANN org's Global Domains Division sent a letter to the GNSO Council requesting input on PPSAI IRT's timeline.

In its response dated 30 April 2019, The GNSO Council deferred to ICANN org and the IRT on questions related to IRT's timeline. In the letter, the Council shared a concern raised by the Registrar Stakeholder Group that there was a need to further clarify the scope of the referral to the PPSAI IRT and to broaden the scope of the compliance deferral. The Council noted that its original request for compliance deferral was too narrow, as it did not cover other use cases and implementation concerns outlined by the RrSG, such as the scenario where there is an "Underlying Registrant Data Change Without Privacy/Proxy Service Change." As a result of the narrow language, the GNSO Council noted that ICANN-accredited registrars experienced significant compliance issues.[21] The Council asked ICANN org to work with the RrSG and other interested parties to clarify the scope of referral to the PPSAI IRT and broaden the compliance deferral.

ICANN org responded to the GNSO Council in a letter dated 5 September 2019, stating that ICANN org continued to believe that the PPSAI implementation work should remain on hold pending the implementation of the EPDP Phase 2 recommendations. ICANN org indicated that it would work with the RrSG on scoping the privacy/proxy issue. Regarding deferrals of compliance enforcement, it recommended that any deferral request be clearly scoped and directed to the ICANN Board in order to enable ICANN org implementation.

At the time of writing this report, issues with Change of Registrant lock as they relate to privacy/proxy services are still under discussion. Implementation of the Privacy and Proxy Service Provider Accreditation Program remains on hold, pending outcomes of related EPDP work on a possible access model for nonpublic gTLD registration data. The PPSAI IRT is expected to continue work on the issue referred from the GNSO Council once the EPDP outcomes are known.

3.1.3.5. Inputs Received in Response to the Transfer Policy Status Report

The Transfer Policy Status Report draws on a number of data points offering evidence that registrants are experiencing challenges with the Change of Registrant policy, and specifically with the 60-day lock. These data points include:

- Data on inquiries handled by ICANN's Global Support Center
- ICANN Aggregate Transfer-Related Monthly Registry Reporting
- Data on complaints handled by ICANN's Contractual Compliance Department
- Responses to the survey launched to support the preparation of the Transfer Policy Status Report.

[21] As an example, see the letter from Tucows to Contractual Compliance dated 19 December 2018 and response from ICANN's Contractual Compliance Department date 1 March 2019.

Global Support Center Inquiries

The Transfer Policy Status Report includes statistics on inquiries handled by ICANN's Global Support Center (GSC), whose dedicated support team receives and provides support for inquiries from registries, registrars, new gTLD applicants, and the Internet community at large.

The Transfer Policy Status Report, on page 47, notes that from 1 January 2015 - 23 May 2018, GSC reported 6,736 inquiries regarding transfers. Of those, 701 inquiries involved a registered name holder who was unable to initiate an inter-registrar transfer due to the 60-day "Change of Registrant" lock. The number of inquiries received regarding transfers increased at a higher rate than the overall amount of inquiries received (which also increased). According to the Transfer Policy Status Report, GSC posited that the increase in transfer-related inquiries is likely due to an increase in issues related to the Change of Registrant (COR) lock (see page 46).

The following are examples of inquiries received by GSC in relation to the 60-day lock, as summarized in Annex 8.1 of the Transfer Policy Status Report:

- Registrar denied transferring a domain, caller believes registrar changed contact information without customers consent now the 60-day lock is in place and is unable to be transferred.
- Registrant wants to transfer domain name, but is in 60-day lock and wants the lock to be removed.
- Registrant thinks 60-day lock was made up by his registrar and wants ICANN to bypass.
- Registrant wants to transfer, but registrar denies transfer due to 60-day lock. User generated own AuthCode through control panel, and finds his domain has disappeared. Asking ICANN for guidance. ICANN responds with noting 60-day lock period.
- Registrant filed complaint against registrar because they weren't receiving AuthCode to transfer domain. Realized they had invalid email account linked to domain, 60-day lock initiated once they changed contact information.

ICANN Aggregate Transfer-Related Monthly Registry Reporting

The Transfer Policy Status Report includes data on trends in transfers from 2009 to 2018, based on an aggregate view of ICANN Monthly Registry Reports that gTLD registries provide to ICANN.

Noting that there are peaks and troughs throughout the reporting period, data indicates that there was a prominent spike in transfers toward the end of 2016. The Transfer Policy Status Report speculates that this spike may be explained by the then forthcoming implementation of the IRTP Part C, including the 60-day lock (see page 18).

Metrics and Input from ICANN Contractual Compliance

The Transfer Policy Status Report analyzed data provided by ICANN's Contractual Compliance Department on tickets received between 2012 and 2018. According to the Report, on page 31: "The nature of transfer complaints changed in December 2016, when the IRTP-C and -D became effective. While inter-registrar transfer complaints have been trending downward, Contractual Compliance noticed an increase in complaints relating to the "Change of Registrant" (COR) lock that became effective in December 2016."

In reflecting on the tickets received in relation the CoR, ICANN org's Contractual Compliance Department identified the following opportunities to enhance the Transfer Policy (see page 32):

- Provide a process or options to remove the 60-day lock to better serve registrants' needs. For example, reporters express frustration about the 60-day lock due to the "Change of Registrant" provision under Section II.A.1.1 of the Transfer Policy. Their frustrations stem from an inability to transfer their domain(s) to a new registrar if the domain is due to expire during the lock period.
- Clarify whether "Change of Registrant" provision applies to customer data when it is used by a privacy/proxy provider as it relates to the 60- day lock.

Survey Inputs

The ICANN org survey conducted to support the preparation of the Transfer Policy Status Report included a number of questions on Change of Registrant. The responses highlight some of the concerns and potential areas for improvement identified by registrars and registrants.

The Transfer Policy Status Report summarizes survey input with respect to Change of Registrant:

- Respondents wanted to see fewer and/or less complicated steps for registrants to transfer their domain(s), and quicker transfer times.
- Respondents express frustration when they encounter barriers to transferring their domain name(s) (e.g. the "Change of Registrant" lock).
- Some respondents recommended eliminating or reducing the 60-day Change of Registrant transfer lock imposed on registrants who've changed their contact information.
- Some registrar respondents indicated that their customers were often frustrated with certain aspects of the Policy, and did not seem to understand the underlying rationale for certain requirements (such as the Change of Registrant lock).

Specific responses to the survey questions offer additional detail on these concerns.

Question 5 of the survey asked: "The transfer policy has evolved over the last six years. In your opinion, have the policy modifications improved, worsened, or had no effect on the process for transferring domains between registrars and/or registrants? Please provide details to support your answer." Responses to this question varied from "complicated" and "worsened" to "simple" and "improved." The RrSG responded: "For Change of Registrant, it's gotten worse. It is overly complicated and a bad user experience."

Question 12 specifically addressed the 60-day lock: "What issues, if any, have you encountered with the 60-day "Change of Registrant" lock requirement? Do you see this as an effective policy requirement? Please explain your answer. Respondents were somewhat ambivalent about the 60-day "Change of Registrant" lock requirement, but gravitated toward lack of support. While acknowledging it helps with the security of transfers, registrars expressed that their customers often did not understand it or viewed it as burdensome, which resulted in more calls to registrar support teams. Some viewed the period as too long. Some representative answers were:

- "[The CoR lock] has been a frustration for registrants and registrars alike. There are many reasons registrants choose to lock or unlock their domains. Automatic locking causes confusion. This often leads to increased contacts from registrants when transfers fail."

- "We support having a delay as it is effective and gives registrants an opportunity to act/respond in cases of fraud. However, forcing parties to accept it has over-complicated the issue. Additionally, overuse of the designated agent has negated the Change of Registrant policy, making it ineffective. Ultimately, the 60-day change of registrant transfer lock should be at the registrar's discretion."
- "The 60-day Change of Registrant lock requirement can at times be a burden, both inbound and outbound. An example would be when a registrant is simply correcting information before a transfer. This also hinders corporate acquisitions and divestitures, as companies are legitimately updating large lists of domains to new legal entities."
- "Many registrants don't understand the 60-day lock policy. So they think that [it] is [an] inconvenience. But [it is] an effective policy requirement."
- "It is not an effective policy because it only traps legitimate registrants; hijackers by now all know to avoid changing the registrant before a hijacking. It should be eliminated."
- "We support the 60-day 'change of registrant' lock requirement. This prevents immediate transfers after a domain has been updated."

The RrSG assigned a score of "3" (out of 10) to the "Change of Registrant" process, stating:

> *The 60 day Change of Registrant lock requirement can at times be a burden when a client wants to transfer the domain to another registrar for an unforeseen reason prior to the end of the 60 days. Registrants who do not opt-out of the lock often don't understand why their domain is locked (despite explanations presented at the time of update). This can create an unnecessary waiting period.*
>
> *The approval delay is effective at giving registrants an opportunity to catch and prevent fraud, but forcing users to accept the transfer is over-burdensome. There is also over-use of the Designated Agent, which has basically circumvented the policy.*
>
> *COR also hinders corporate acquisitions, consolidations, and divestitures of large lists of domains to new legal entities, which places the domains in a lock that can then be problematic.*

Question 14 of the survey asked: "When implementing "Change of Registrant" lock requirement, did you choose to implement the opt-in option vs. the opt-out? Why or why not?" Responses and rationales were split on this question. "Opt-in" respondents indicated they did so to increase security, while "opt-out" respondents did so for the sake of simplifying the transfer process for their customers. Others provided their customers with the choice, for example:

- "Opt-in for greater protection" and "for security purposes."
- "We chose opt-out by default. The 60-day Change of Registrant lock requirement can at times be a burden, both inbound and outbound. An example would be when a registrant is simply correcting information before a transfer."
- "We give the option to select either. We do not default to one or the other. We allow the customers to choose."

Question 15 asked: "Should the duration of the "Change of Registrant" lock stay the same, or be shorter, longer, or no longer a requirement?" Of the 34 responses received, 16 (47.06%) responded that it

should no longer be a requirement. Nine (26.47%) responded that it should be the same. Six (17.65%) responded that it should be shorter. Three (8.82%) responded that it should be longer.

Question 19 asked registrars: "In general, what issues are your customers having, if any, as they relate to transfers?" Some of the responses addressed CoR, for example:

- ". . . Customers hate the Change of Registrant policy. . ."
- "Contact updates leading to inadvertent blocking of legitimate transfers. That's by far the #1 problem."
- "Registrants are frustrated by the automatic lock. . ."

Additional comments from registrars on this topic include the following:

- In response to question 21, which asked, "What do you think the ideal transfer process should look like from a policy and technical perspective?" one registrar replied: ". . . modify, reduce, or remove lock requirements."
- In response to question 23, which asked, "In your view, what could be improved in regard to making domain name transfers?" one registrar answered: "Remove the change of registrant requirements as they have no impact to domain hijacking."
- In response to question 24, which asked, "If you have any additional input on the IRTP and/or transfer process in general, please do so here." one registrar responded: "The requirements around changes of ownership had good intentions but are incredibly frustrating for registrants. It is a policy that is almost impossible to implement in a customer-friendly way."
- The RrSG recommended the following: "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."

Survey questions directed at registrants resulted in feedback that largely echoed issues raised by registrars. In response to a question about their experience with transferring domain names from one registrar to another (question 25), some respondents raised issues with the 60-day lock when there is a Change of Registrant in conjunction with the inter-registrar transfer. For example:

- "...I would characterize transferring from one registrar to another for a novice [registered name holder] to be difficult as there used to be several emails involved to process a transfer if they needed to make any contact changes on the registrant details. Then after that is done, more potential email and waiting."
- "...I would rather not have the 60-day wait period for inter-registrar domain transfers or change of registrant contact."

The survey asked registrants in question 26, "How would you characterize your experience transferring your domain name(s) from one registrant to another?" Seven respondents (31.82%) said "very easy." Six (27.27%) responded they found the process "neither easy nor difficult." Two respondents (9.09%) responded "very easy" and another two (9.09%) responded "difficult." One registrant (4.55%) found the process "very difficult." An example of a detailed answer: "I find this very difficult now due to the change of registrant process. Reputable registrars have security measures in place outside of the transfer process itself in order to prevent hijacking and those need to be entrusted."

When asked in question 28, "In your view, what could be improved in regard to making domain name transfers?" one registrant replied, "I like the current process, [but] add the [Change of Registrant requirement] back in for gaining registrars."

ICANN Complaints Office

The Transfer Policy Status Report notes that one complaint received from a registrant by ICANN org's Complaints Office provides an illustrative example of a registrant's experience with the 60-day lock. The registrant's registrar had an old email address for the registrant. When the registrant decided to transfer the domain, he realized his original registrar had the old email, which he could not access, and thus could not receive the AuthInfo Code to authorize the transfer to a new registrar. When he updated his email in the registration data directory, the 60-day lock was imposed. The registrant complained that this put him in a "catch-22" situation in which he "wasn't able to transfer the domain without changing an email address, but doing so would prevent [him] from transferring the domain."[22]

The Transfer Policy Review Scoping Team noted in their report that the above-described scenario is common. Registrants "clean-up" their contact data before transferring domains between registrars, and do not understand why a change to the registrant information should trigger a transfer process action such as Change of Registrant.

3.1.3.6. Additional Input from ICANN Contractual Compliance

In the development of this report, ICANN org's Contractual Compliance Department identified additional areas of the Transfer Policy that may be appropriate to review based on complaints received.

- The Transfer Policy defines "Designated Agent" as an individual or entity that the Prior Registrant or New Registrant explicitly authorizes to approve a Change of Registrant on its behalf. Through the processing of complaints received under the Transfer Policy, ICANN org's Contractual Compliance Department has observed broad and extensive use of the Designated Agent role to approve CORs, with the Designated Agent being the registrar or reseller, and the explicit authorization being given through a clause added to the registration agreement. While this is not prohibited by the Transfer Policy, Contractual Compliance has observed that there appear to be different interpretations of the role and authority of the Designated Agent. The following are examples of scenarios observed in complaints:
    - A reseller receives a request for the AuthInfo code and unlocking from the Registered Name Holder. The reseller then initiates and consents to a COR, changing the registrant's contact information to the reseller's own. This effectively prevents the customer from being able to transfer and ultimately from being listed as the registrant of the domain name. According to the Registration Agreement, the reseller is the Designated Agent and is using this role to perform the COR. In this case, the interpretation appears to be that the authority of the Designated Agent includes initiating a COR that was not requested or wanted by the Registered Name Holder.
    - A reporter/Registered Name Holder asks the reseller to change the Registrant Email in order to obtain the AuthInfo code. The reseller, as the Designated Agent, consents to the COR and the Prior Registrant is not provided the option to opt-out of the 60-day COR (if the option is provided). Since the warning regarding the COR lock may be

[22] Transfer Policy Status Report page 18.

provided to the Designated Agent, the Registered Name Holder only becomes aware of the 60-day COR lock after the COR is completed and the lock is implemented.

- ICANN Contractual Compliance has received complaints in which the complainants claimed that they were never advised of the 60-day COR lock. In at least one instance, the registrar responded to the Compliance inquiry that the notification of the COR lock is provided via the Terms of Service/Registration Agreement between the Registered Name Holder and the registrar/reseller. This may provide an indication that it would be helpful to review Section II.C.1.3 of the Transfer Policy, which describes how the information about the lock must be provided.
- ICANN Contractual Compliance has received complaints from new registrants who purchased domain names from the "Prior Registrants" and have complained that they (the "New Registrants") have not been provided the option to opt-out even though the registrar/reseller provides that option. This may provide an indication that it would be helpful to clarify in Section II.C.2 that the option to opt-out is provided only to the Prior Registrant.

3.1.3.7. Further Policy Questions for Consideration

Change of Registrant - Overall Policy

1. 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?
2. 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?
3. 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.

60-Day Lock

4. 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?
5. 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?
6. 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?
7. 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?
8. 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 ~~Registered Name Holder~~ **Prior Registrant** to opt out of the 60-day inter-registrar transfer lock prior to any Change of Registrant request."?

Change of Registrant - Privacy/Proxy Customers

9. 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.[23] Are there additional scenarios that need to be considered that are not included in this list?
10. 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?
11. Are notifications provided to privacy/proxy customers regarding COR and changes to the privacy/proxy service information sufficient? For example, should 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?

Designated Agent

12. 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?
13. If the Designated Agent function is not operating as intended, should it be retained and modified? Eliminated?
14. Are there alternative means to meet the objectives of Designated Agent role?
15. 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?
16. 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

17. 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?

[23] 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

3.1.4. Transfer Emergency Action Contact ("TEAC")

3.1.4.1. Overview of Existing Provisions Regarding the Transfer Emergency Action Contact

According to Section I. A.4.6 the Transfer Policy, registrars are required to designate a Transfer Emergency Action Contact (TEAC) to "facilitate urgent communications relating to transfers" with the goal of "quickly establish[ing] a real-time conversation between registrars (in a language that both parties can understand) in an emergency." Communications to TEACs are reserved for use by ICANN-Accredited Registrars, gTLD Registry Operators, and ICANN org (Section I.A.4.6.2).

Provisions regarding the TEAC include the following:

- The TEAC point of contact may be designated as a telephone number or some other real-time communication channel (Section I.A.4.6.2).
- Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain (Section I.A.4.6.2).
- Messages sent via the TEAC communication channel must generate a non-automated response by a human representative of the Gaining Registrar (Section I.A.4.6.3).
- The person or team responding must be capable and authorized to investigate and address urgent transfer issues (Section I.A.4.6.3).
- Responses are required within 4 hours of the initial request, although final resolution of the incident may take longer (Section I.A.4.6.3).

The policy further specifies consequences for the registrar if a TEAC does not respond in the specified timeframe: "Failure to respond to a TEAC communication may result in a transfer-undo . . . and may also result in further action by ICANN, up to and including non-renewal or termination of accreditation" (Section I.A.4.6.4). According to the policy, both parties will retain correspondence in written or electronic form of any TEAC communication and responses, and will share copies of this documentation with ICANN and the registry operator upon request (Section I.A.4.6.5).

Section I.A.6.4 of the policy states that the registry operator shall undo a transfer if, after a transfer has occurred, the registry operator receives documentation provided by the Registrar of Record prior to transfer that the Gaining Registrar has not responded to a message via the TEAC within the timeframe specified by the policy (section I.A.6.4.4). The registry operator must undo the transfer within five (5) calendar days of receipt of the notice.

Registrars currently access TEAC information through ICANN's Naming Services Portal, which replaced the Registrar Application and Data Access Resource (RADAR) platform on 28 October 2019.

3.1.4.2. Previous Policy Work Regarding Transfer Emergency Action Contact

TEAC requirements in the Transfer Policy stem from Recommendation #1 in the IRTP Part B PDP Working Group's Final Report.

The IRTP Part B PDP Working Group was tasked with addressing five issues related to domain name hijacking, including the following, as identified in the Final Issue Report:

(1) Whether a process for urgent return/resolution of a domain name should be developed, as discussed within the SSAC hijacking report.

The IRTP Working Group ultimately concluded that such a process should be developed, and that registrars should be required to designate a Transfer Emergency Action Contact as part of this process. Recommendation 1 in the Final Report states: "The Working Group recommends requiring registrars to provide a Transfer Emergency Action Contact (TEAC)" and provides proposed text to add to Inter-Registrar Transfer Policy.[24]

In its deliberations on this topic, summarized in Part B of the Final Report, the Working Group reviewed the SSAC's report Domain Name Hijacking: Incidents, Threats, Risks and Remedial Actions (SAC007), as well as Measures to Protect Domain Registration Services Against Exploitation or Misuse (SAC040). The Working Group agreed that there is value in having processes in place to address urgent return/resolution of a domain name. Several of the registrars participating in the Working Group pointed out that in practice, registrars work together to solve these kinds of situations, but it was noted that an escalation process might be desirable in cases where a registrar would be unresponsive or unwilling to cooperate.

Initially, the Working Group considered whether the Transfer Dispute Resolution Process (TDRP) could be adapted to address urgent concerns. The Working Group decided that this was not an appropriate course of action, noting that the TDRP is slow, resource intensive, and rarely used. The Working Group later considered a proposal for an Expedited Transfer Reverse Procedure (ETRP), but after reviewing public comments on the proposal, decided that it was too complicated and could generate severe unintended consequences.

The Working Group deliberated on the concept of a TEAC, which was proposed in SAC007. The Working Group requested community input through public comment on a number of questions related to the TEAC, including how quickly a TEAC should be expected to respond, what qualifies as a "response," whether there should be consequences if a TEAC does not respond in the specified timeframe, and who can use the TEAC.

The Working Group put together a detailed proposal in its Final Report, taking into account the input received through public comment. In its Implementation Recommendations, the Working Group stated that a review of the TEAC should be conducted 12 to 24 months after implementation of the policy to address whether the TEAC is working as intended, whether the TEAC is not abused, and whether the option to 'undo' a transfer in the case of failure to respond to a TEAC should be made mandatory.

The Working Group's recommendation was implemented by adding the definition and requirements of the Transfer Emergency Action Contact into Section I.A.4.6 of the Transfer Policy. The policy effective date was 1 June 2012.

3.1.4.3. Input Received in Response to the Policy Status Report

The ICANN org survey conducted to support the preparation of the Transfer Policy Status Report included one question specifically addressing the TEAC. In addition, responses to more general survey questions included comments regarding the TEAC.

[24] For the proposed text, see pages 4-6 of the Final Report.

Question 18 of the survey specifically addressed the TEAC and asked, "Do you think the Transfer Emergency Action Contact ("TEAC") is an effective way to handle urgent inter-registrar transfer issues between registrars, or does the TEAC process require changes?" Of the 25 responses received to this question, a number of responses indicated that they were unfamiliar with the TEAC or that they rarely or never used the TEAC. Among those responses that indicated familiarity with the TEAC, some answered that the TEAC was effective while others indicated that the process requires changes.

A key theme in the comments was concern about the requirement that registrars must respond to communications via the TEAC channel within four hours. The RrSG provided a detailed statement on this issue:

". . .There is significant concern with the 4-hour response time requirement, as this can be a burden especially across different time zones and languages. One option could be to require the current 4-hour response time for registrars with overlapping time zones, while registrars with significant disparities in time zone could have a longer response time."

One of the additional commenters on this issue suggested that the TEAC response time should be extended to 12-24 hours.

Several comments provided feedback that TEAC should be part of a broader process with clear timeframes for resolving issues. The RrSG stated:

"The TEAC is an effective way to make contact regarding an urgent transfer issue, but it does not go far enough, because it does not require that both registrars work together to investigate and reverse the disputed transfer if needed. The process should be revised to require the two registrars to come to a mutually acceptable resolution, potentially with the assistance of a neutral mediator."

Other inputs on this topic:

- "...registrars need to be required to respond to all inquiries and find resolution (whatever it may be) and not just an initial response within 4 hours. We would like to see TEAC be the start of a process requirement where both registrars work to come to a resolution."
- "What is needed is a deadline by which a TEAC response must give a final answer on whether the transfer will be reversed, not merely a deadline on when they have to send a generic useless response."

One additional response noted the importance of ensuring that registrars keep their TEAC information up to date.

In addition to comments in response to Question 18, input about TEAC was also submitted in response to some of the more general survey questions.

For example, a respondent indicated that the TEAC 4-hour response time is unfair to registrars in different time zones in response to Question 5, which states: "The transfer policy has evolved over the last six years. In your opinion, have the policy modifications improved, worsened, or had no effect on the process for transferring domains between registrars and/or registrants? Please provide details to support your answer."

Question 16 asked: "Should there be more standard reporting requirements across registrars as they relate to transfers? If so, what should these reporting requirements include?" One response proposed reporting requirements with respect to the TEAC: "We might want to check how often the [Transfer Emergency Contact] is used to assess if it is effective."

Question 29 targeted registrants and asked them for additional input of the IRTP and transfer process, in general. One response stated: "ICANN should define clearly [the] resolving procedures for transfer abuse in the transfer policy."

3.1.4.4. Further Policy Questions for Consideration

1. Is additional data needed to support evaluation of the effectiveness of the TEAC mechanism? If so, what data is needed?
2. The time frame (4 hours) for registrars to respond to communications via the TEAC channel has been raised as a concern by the Transfer Policy Review Scoping Team and in survey responses. Some have expressed that registries must, in practice, have 24x7 coverage by staff members with the appropriate competency to meet this requirement and the language skills to respond to communications from around the world. Is there merit to concerns that the requirement disproportionately impacts certain registrars, namely:
    a. Registrars located in regions outside of the Americas and Europe, because of significant time zone differences?
    b. Small and medium-sized registrars, which may not have a sufficiently large team to have 24x7 staff coverage with the necessary competency?
    c. Registrars in countries where English is not the primary language, who may, in practice, need to have English-speaking TEAC contacts to respond to requests in English?

    To what extent should the 4-hour time frame be revisited in light of these concerns? Are there alternative means to address the underlying concerns other than adjusting the time frame?
3. Section I.A.4.6.2 of the Transfer Policy states that "Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain." The Transfer Policy Review Scoping Team noted that this timeframe should be more clearly defined. Is additional guidance needed to define a "reasonable period of time" after which registrars should be expected to use a standard dispute resolution process?
4. According to section I.A.4.6.2 of the Transfer Policy, the TEAC may be designated as a telephone number, and therefore some TEAC communications may take place by phone. The Transfer Policy Review Scoping Team flagged this provision as a potential item for further consideration. Do telephone communications provide a sufficient "paper trail" for registrars who may later wish to request a transfer "undo" based on failure by a TEAC to respond? Such a request would require the registrar to provide evidence that a phone call was made and not answered, or a call back was not received within 4 hours. Noting this requirement, should the option to communicate by phone be eliminated? Is an authoritative "system of record" for TEAC communications warranted? If so, what are the requirements for such a system?
5. The Transfer Policy Review Scoping Team indicated that there are several factors that make a Registry Operator's obligation to "undo" a transfer under Section 6.4 of the Transfer Policy challenging:
    a. Registry Operators do not have access to the designated TEACs for each Registrar, making validation of an undo request nearly impossible.

b. There is no way for Registry Operators to independently verify that a Registrar did not respond within the required time frame or at all since Registry Operators are not a party to, or copied on, communications between the Registrar TEACs.
c. Transfer "undo" requests associated with the failure of a TEAC to respond are unilateral so there is no validation required prior to a Registry Operator taking action. This has, on occasion, led to a "he said", "she said" scenario.
d. Follow on to 4.c., if the policy were to be updated to allow for some level of validation by the Registry Operator prior to taking action, the requirement to "undo" a transfer within 5 calendar days of receiving an TEAC undo request leaves little to no time to attempt to validate the request prior to taking the action.

To what extent are changes to the policy needed to address these concerns? Are there other pain points for Registry Operators that need to be considered in the review of the policy in this regard?

3.1.5. Transfer Dispute Resolution Policy ("TDRP")

3.1.5.1. Overview of the Transfer Dispute Resolution Policy

In any dispute relating to inter-registrar domain name transfers, registrars are encouraged to first attempt to resolve the problem among the registrars involved in the dispute. In cases where this is unsuccessful and where a registrar elects to file a dispute, the Transfer Dispute Resolution Policy (TDRP) details the requirements and process to do so.

There are two dispute resolution providers approved by ICANN to consider TDRP complaints. Registrars file disputes directly with these providers:

- The Asian Domain Name Dispute Resolution Centre (ADNRC)
- The National Arbitration Forum (NAF)

The following summarizes key elements of the procedure:

- A dispute must be filed no later than twelve (12) months after the alleged violation of the Transfer Policy (Section 2.2). The complainant may be either a Losing Registrar (in the case of an alleged fraudulent transfer) or a Gaining Registrar (in the case of an improper NACK) (Section 1.1).
- The complainant submits the complaint and supporting documentation to the dispute resolution provider (Section 3.1).
- The respondent submits a response to the complaint within seven (7) calendar days (Section 3.2).
- The dispute resolution provider panel must reach a conclusion no later than thirty (30) days after receipt of response from the respondent (Section 3.2.4).
- Resolution options for the dispute resolution panel are limited either approving or denying the transfer (Section 3.2.4.v). The dispute resolution panel may not issue a finding of "no decision." It must weigh the applicable evidence in light of the Transfer Policy and determine, based on a preponderance of the evidence, which registrar should prevail in the dispute and what

resolution to the complaint will appropriately redress the issues set forth in the complaint (section 3.2.4.iv).
- The TDRP does not prevent a registrar from submitting a dispute to a court of competent jurisdiction for independent resolution before the administrative proceeding is commenced or after it is concluded (section 3.4).

The dispute resolution providers maintain supplemental rules covering topics such as fees, word and page limits and guidelines, the means for communicating with the provider, and the form of cover sheets. These supplemental rules are published on the ADNDRC and NAF websites.

3.1.5.2. Previous Policy Work on the TDRP

When the Inter-Registrar Transfer Policy (IRTP) was adopted as GNSO consensus policy in 2004, it included the Transfer Dispute Resolution Policy (TDRP) as a mechanism for resolving disputes between registrars in cases of alleged violations of the IRTP.[25]

A number of issues regarding the TDRP were among those topics identified for further work by the Transfer Policy Group in 2007. These issues were the focus of the IRTP Working Group Part D Policy Development Process (PDP).

The IRTP Part D PDP Working Group was tasked with addressing six issues, five of which related to the TDRP, as described in the Final Issue Report:

1. Whether reporting requirements for registries and dispute providers should be developed, in order to make precedent and trend information available to the community and allow reference to past cases in dispute submissions;
2. Whether additional provisions should be included in the TDRP (Transfer Dispute Resolution Policy) on how to handle disputes when multiple transfers have occurred;
3. Whether dispute options for registrants should be developed and implemented as part of the policy (registrants currently depend on registrars to initiate a dispute on their behalf);
4. Whether requirements or best practices should be put into place for registrars to make information on dispute resolution options available to registrants;
5. Whether existing penalties for policy violations are sufficient or if additional provisions/penalties for specific violations should be added into the policy.

The following is an overview of the Working Group's recommendations related to the TDRP, as summarized in the Transfer Policy Status Report:

- Recommendation 1: The Working Group recommends that reporting requirements be incorporated into the Transfer Dispute Resolution Policy.
- Recommendation 2: The Working Group recommends that the Transfer Dispute Resolution Policy be amended to include language regarding the publication of decisions.[26]

[25] See Annex A of the Final Issue Report on the Inter-Registrar Transfer Policy Part D for language included in the TDRP prior to the policy work conducted as part of IRTP Part D.
[26] The Working Group recommended specific language to be included in Transfer Dispute Resolution Policy. For more information, see the IRTP D Working Group's Final Report, p 18: https://gnso.icann.org/sites/default/files/filefield_46639/irtp-d-final-25sep14-en.pdf.

- Recommendation 3: The Working Group recommends that the Transfer Dispute Resolution Policy be amended to ensure that transfers from a Gaining Registrar to a third registrar, and all other subsequent transfers, are invalidated if the Gaining Registrar acquired sponsorship from the Registrar of Record through an invalid transfer.
- Recommendation 4: The Working Group recommends that the Transfer Dispute Resolution Policy be amended to specify that a domain name must be returned to the Registrar and Registrant of Record directly prior to the non-compliant transfer.
- Recommendation 5: The Working Group recommends that the statute of limitation to launch a Transfer Dispute Resolution Policy be extended to 12 months from the initial allegedly invalid transfer.
- Recommendation 6: The Working Group recommends that if a request for enforcement is initiated under the Transfer Dispute Resolution Policy or a Uniform Rapid Suspension action, the relevant domain should be locked against further transfers while such request for enforcement is pending.
- Recommendation 7: The Working Group recommends adding a list of definitions (Annex F) to the Transfer Dispute Resolution Policy.[27]
- Recommendation 8: The Working Group does not recommend the addition of dispute options for registrants as part of the current Transfer Dispute Resolution Policy.
- Recommendation 9: The Working Group recommends that ICANN, in close cooperation with the IRTP Part C Implementation Review Team, monitor whether dispute resolution mechanisms are necessary for the Change of Registrant function.
- Recommendation 10: The Working Group recommends eliminating the First Level (Registry) of the Transfer Dispute Resolution Policy.
- Recommendation 11: The Working Group recommends that ICANN take the necessary steps to display information relevant to disputing non-compliant transfers prominently on its website and ensure the information is presented in a simple and easy-to-understand manner for a registrant audience.
- Recommendation 12: The Working Group recommends that ICANN create and maintain a user-friendly, one-stop website containing all relevant information concerning disputed transfers and potential remedies to registrants.
- Recommendation 13: The Working Group recommends that, as a best practice, ICANN-accredited Registrars prominently display a link on their website to this ICANN registrant help site.
- Recommendation 14: The Working Group recommends that no additional penalty provisions be added to the existing Inter-Registrar Transfer Policy or Transfer Dispute Resolution Policy.
- Recommendation 15: The Working Group recommends avoiding policy-specific sanctions wherever possible.

Several key elements of the IRTP Part D Working Group's deliberations from the Final Report are summarized here for ease of reference.

[27] The Working Group recommended specific definitions be included Transfer Dispute Resolution Policy. For more information, see the IRTP D Working Group's Final Report, Annex F: https://gnso.icann.org/sites/default/files/filefield_46639/irtp-d-final-25sep14-en.pdf.

The IRTP Part D Working Group's Recommendation 5 resulted in the extension of the statute of limitations to initiate a TDRP from 6 months to 12 months. In its deliberations, the Working Group noted that many registrants do not regularly check the status of their domain names, and therefore 6 months may not be long enough to notice a disputable transfer and notify the registrar, who in turn would need to initiate a dispute. The Working Group considered registrars' obligation under the Whois Data Reminder Policy (WDRP) to contact registrants annually, and noted that an extension to 12 months may be desirable in this regard. According to the Working Group's Final Report, the extension could "mitigate multi-hop transfer problems by providing the losing registrant additional 'reaction time' to inquire with their registrar after they did not receive their annual reminder to update their contact information." In addition, the Working Group did not believe that that extension unduly burdened legitimate transfers.

The Working Group considered whether there should be dispute resolution options for registrants under the TDRP and ultimately determined that such options should not exist, as stated in the Final Report's Recommendation 8. In deliberations, the Working Group raised concern that adding a new class of parties to the TDRP would overload the mechanism. Further, the Working Group noted that it was unclear how the "loser-pays" model could work when the two parties to the dispute are a legitimate registrant and a criminal. The Working Group discussed that a mechanism may be needed in the future to address disputes resulting from inter-registrant transfers, but that such a need should be re-evaluated after the implementation of IRTP Part-C recommendations and analysis of relevant data. As a result of this discussion, the Working Group put forward Recommendation 9, which stated that CANN should monitor whether dispute resolution mechanisms are necessary for the Change of Registrant function.

The Working Group reviewed the two "level" approach to the TDRP that was in place at the time that the Working Group conducted its review of the policy. At the time, registrars had two possible options for filing a transfer dispute:

1. File a dispute with the relevant Registry Operator (first level)
2. File a dispute with a Dispute Resolution Panel (second level)

The second level filing could be used as the first option or as an appeal to a first level ruling. If it was used as the first option, the registrar could not go back to the first level.

In its deliberations, the Working Group discussed that removing the registry level could increase costs for registrars, and possibly registrants, because filing with dispute resolution providers was more expensive than filing with registries. They noted that higher costs could result in reluctance to file disputes. The Working Group considered the small number of disputes initiated and the fact that registrars would continue to have the option to come to agreement before initiating a formal dispute, and concluded that it was unlikely that there would be a significant increase in costs. The Working Group discussed the benefits to eliminating the registry layer, including a more consistent application of the process, because a smaller number of entities would process disputes, as well as reduced costs for registries who would no longer need to maintain dispute resolution capabilities. The Working Group determined that, on balance, it was appropriate to eliminate the registry as a first-level dispute resolution provider in the TDRP process, and therefore included this guidance in Recommendation 10.

The Working Group's recommendations were adopted by the GNSO Council on 15 October 2014 and adopted by the ICANN Board on 12 February 2015. Policy recommendations were implemented through

a series of updates to the TDRP,[28] which went into effect on 1 December 2016. In addition, a dedicated Transfers page was added under the Registrants sections of ICANN's website as part of the implementation of Recommendations 11-13, which focus on accessibility of information.

3.1.5.3. Inputs Received in Response to the Policy Status Report

Survey Inputs

The ICANN org survey conducted to support the preparation of the Transfer Policy Status Report included a number of responses that addressed the TDRP and additional input on dispute resolution more broadly.

Question 1 of the survey requested input from registrars on the efficacy of the Transfer Policy and asked: "On a scale of 1 to 10, how effective is the transfer policy generally as it exists today (10 being most effective)?"

The Registrar Stakeholder Group responded to this question with a "6 or 7" for the Transfer Policy overall, but ranked the dispute process at "0," stating "The Dispute policy is ineffective. It cannot be used at this time to reverse a transfer, so that section of the policy gets a 0."

Responses to additional questions point to concerns that registrants have limited options to address disputes regarding illegitimate transfers.

For example, in response to question 5, which asked registrars whether policy modifications have improved, worsened, or had no effect on the process for transferring domains between registrars and/or registrants, one of the responses stated: "For registrants it is overly complicated and a bad experience. This is primarily due to issues with fraudulent transfers and not having effective and efficient means to address them."

Question 19 asked registrars what issues their customers are facing. One of the responses noted that ". . . in general a lack of good dispute mechanisms" was a problem. In response to this question, the Registrar Stakeholder Group provided input that ". . . If a domain is hijacked, there is no effective dispute or resolution mechanism. . ."

Question 21 stated: "What do you think the ideal transfer process should look like from a policy and a technical perspective?" One of the responses stated: "Effective and accessible dispute mechanism that puts the burden of proof on the gaining registrar and the requesting registrant."

3.1.5.4. Disputes Filed Under the TDRP

Disputes Logged by Registry Operators

The Transfer Policy Status Report includes data on transfer dispute cases from 2010-2017 (see page 12). Until 1 December 2016, when IRTP Part D recommendations went into effect and the first (registry) level of disputes was eliminated, registry operators logged transfer disputes as part of their Specification 3 reporting. The Transfer Policy Status report noted a spike in Transfer Dispute Resolution Policy (TDRP)

[28] Summarized on pages 67-72 of the Transfer Policy Status Report.

cases in 2015, but observed that the number of cases was still relatively small compared to the total amount of transfers that occurred.

Disputes Filed with Dispute Resolution Providers

As part of its analysis, the IRTP Part D Working Group solicited input from the National Arbitration Forum (NAF) and Asian Domain Name Dispute Resolution Centre (ADNDRC) for additional information on TDRP cases that they had processed to date. The following summary is excerpted from the IRPT Part D Final Report:

> *The NAF has processed 6 TDRP cases:*
> - *All 6 were appeals of first level decisions and concerned Verisign-administered domains*
> - *At the first level (of those 6 cases), the gaining registrar prevailed once, one request was denied and four resulted in no-decision*
> - *At the second level (NAF) the appellant prevailed in 5 cases and the appellee prevailed in 1 case of these cases were fraudulent transfers and 1 case was an attempted transfer*
>
> *The ADNDRC has processed 4 TDRP cases:*
> - *Procedural problems occurred in all four cases*
> - *In all 4 cases the appellee failed to provide sufficient information or any information at all.*
> - *In 2 cases the appellant failed to provide sufficient information*
> - *This resulted in only one case being arbitrated – with the appellant prevailing*
> - *In 2 cases no-decision was rendered, in 1 case the ADNDRC determined that it had no jurisdiction to render a decision.*

Websites for the National Arbitration Forum and Asian Domain Name Dispute Resolution Centre provide publicly-available information about the TDRP cases processed to date. The Transfer Policy Status Report includes, in Annex 8.4, summaries of cases obtained from the dispute resolution providers' websites to provide a deeper look into the details of a transfer dispute.

3.1.5.5. Further Policy Questions for Consideration

1. Is there enough information available to determine if the TDRP is an effective mechanism for resolving disputes between registrars in cases of alleged violations of the IRTP? If not, what additional information is needed to make this determination?
2. The ADNDRC reported to the IRTP Part D Working Group that in some of the cases it processed, appellees and appellants failed to provide sufficient information to support arbitration. Is this an issue that needs to be examined further in the context of the policy?
    a. Are the existing informational materials about the TDRP sufficient to ensure that registrars understand the process and the requirements for filing a dispute, including the information they need to give to the dispute resolution provider?
3. If the TDRP is considered to be insufficient:
    a. Are additional mechanisms needed to supplement the TDRP?
    b. Should the approach to the TDRP itself be reconsidered?
4. Are requirements for the processing of registration data, as specified in the TDRP, compliant with data protection law?

5. Are requirements for the processing of registration data, as specified in the TDRP, appropriate based on principles of privacy by design and data processing minimization?

3.1.6. Denying Transfers

3.1.6.1. Background of Denying (NACKing) Transfers

The Transfer Policy Review Scoping Team noted, in its suggestion of topics for review, that there is confusion over the denial (also referred to as the NACKing) of transfers.

Section I.A.3.7 of the Transfer Policy provides that the Losing Registrar may deny, or NACK, a registrant's inter-registrar transfer request in the following specific instances:

- 3.7.1 Evidence of fraud.
- 3.7.2 Reasonable dispute over the identity of the Registered Name Holder or Administrative Contact.
- 3.7.3 No payment for previous registration period (including credit card charge-backs) if the domain name is past its expiration date or for previous or current registration periods if the domain name has not yet expired. In all such cases, however, the domain name must be put into "Registrar Hold" status by the Registrar of Record prior to the denial of transfer.
- 3.7.4 Express objection to the transfer by the authorized Transfer Contact. Objection could take the form of specific request (either by paper or electronic means) by the authorized Transfer Contact to deny a particular transfer request, or a general objection to all transfer requests received by the Registrar, either temporarily or indefinitely. In all cases, the objection must be provided with the express and informed consent of the authorized Transfer Contact on an opt-in basis and upon request by the authorized Transfer Contact, the Registrar must remove the lock or provide a reasonably accessible method for the authorized Transfer Contact to remove the lock within five (5) calendar days.
- 3.7.5 The transfer was requested within 60 days of the creation date as shown in the registry Whois record for the domain name.
- 3.7.6 A domain name is within 60 days (or a lesser period to be determined) after being transferred (apart from being transferred back to the original Registrar in cases where both Registrars so agree and/or where a decision in the dispute resolution process so directs). "Transferred" shall only mean that an inter-registrar transfer has occurred in accordance with the procedures of this policy.

Section I.A.3.8 of the Transfer Policy provides that the Losing Registrar must deny (NACK) a registrant's inter-registrar transfer request in the following specific instances:

- 3.8.1 A pending UDRP proceeding that the Registrar has been informed of.
- 3.8.2 Court order by a court of competent jurisdiction.
- 3.8.3 Pending dispute related to a previous transfer pursuant to the Transfer Dispute Resolution Policy.
- 3.8.4 URS proceeding or URS suspension that the Registrar has been informed of.

- 3.8.5 The Registrar imposed a 60-day inter-registrar transfer lock following a Change of Registrant, and the Registered Name Holder did not opt out of the 60-day inter-registrar transfer lock prior to the Change of Registrant request.

Section I.A.3.9 of the Transfer Policy also provides specific instances where the Losing Registrar cannot deny a registrant's inter-registrar transfer request:

- 3.9.1 Nonpayment for a pending or future registration period.
- 3.9.2 No response from the Registered Name Holder or Administrative Contact.
- 3.9.3 Domain name in Registrar Lock Status, unless the Registered Name Holder is provided with the reasonable opportunity and ability to unlock the domain name prior to the Transfer Request.
- 3.9.4 Domain name registration period time constraints, other than during the first 60 days of initial registration, during the first 60 days after a registrar transfer, or during the 60-day lock following a Change of Registrant pursuant to Section II.C.2.
- 3.9.5 General payment defaults between Registrar and business partners / affiliates in cases where the Registered Name Holder for the domain in question has paid for the registration.

Section I.A.6 of the Transfer Policy provides specific instances where a Registry Operator may reverse or undo a completed inter-registrar transfer:

- 6.4.1 Agreement of the [Losing Registrar] and the Gaining Registrar sent by email, letter or fax that the transfer was made by mistake or was otherwise not in accordance with the procedures set forth in this policy;
- 6.4.2 The final determination of a dispute resolution body having jurisdiction over the transfer; or
- 6.4.3 Order of a court having jurisdiction over the transfer;
- 6.4.4 Documentation provided by the [Losing Registrar] prior to transfer that the Gaining Registrar has not responded to a message via the TEAC within the timeframe specified in Section I.A.4.6.

For more information on the Transfer Dispute Resolution Policy, under which a registrar may challenge an alleged improper transfer, please refer to Section 3.1.5 of this Report.

3.1.6.2. Previous Policy Work on Denying and Reversing Transfers

GNSO Council Transfer Policy Task Force

In its review of domain name portability in 2003, the GNSO Council Transfer Policy Task Force submitted two consensus policy recommendations regarding instances when the Losing Registrar may deny a

registrant's inter-registrar transfer request. Recommendation 24 and Recommendation 25 from the Transfers Task Forces Final Report is excerpted below for ease of reference:

> ***Recommendation 24****: A Losing Registrar may deny transfer requests only in specific instances and that there should be a finite list of allowable reasons for denying a transfer request with the understanding that procedures should be put into place to modify the list if registrars support changes to the list, and that such changes be approved by ICANN staff, or another equally appropriate body, and that in the event that the changes requested constitute new policy, or are not otherwise authorized by ICANN staff or the appropriate body, that the matter be referred to the GNSO Names Council for consideration. Further that, upon denying a transfer request for any reason, registrars must provide the registrant and the other registrar the reason for denial. Therefore, a Losing Registrar may deny a transfer request only in the following instances;*
>
> *a. Evidence of fraud*
> *b. UDRP action*
> *c. Court order*
> *d. Reasonable dispute over the identity of the Registrant or Administrative Contact*
> *e. No payment for previous registration period (including credit card charge-backs) if the domain name is past its expiration date or for previous or current registration periods if the domain name has not yet expired. In all such cases, however, the domain name must be put into "Registrar Hold" status by the Losing Registrar prior to the denial of transfer.*
> *f. Express written objection from the Registrant or Administrative contact. (e.g. – email, fax, paper document or other processes by which the Registrant has expressly and voluntarily objected through opt-in means)*
> *g. domain name is in lock status provided that the registrar provides a readily accessible and easy means for the registrant to remove the lock status.*
> *h. A domain name is in the first 60 days of an initial registration period.*
> *i. A domain name is within 60 days (or a lesser period to be determined) after being transferred (apart from a transfer back to the original registrar).*
>
> ***Recommendation 25****: Instances when the Losing Registrar may not deny a transfer include, but are not limited to:*
>
> *a. Nonpayment for a pending or future registration period*
> *b. No response from the Registrant or Administrative contact unless the Losing Registrar shows evidence of express written objection from the Registrant or Administrative Contact. (e.g. – email, fax, paper document or other processes by which the Registrant has expressly and voluntarily objected through opt-in means)*
> *c. Domain name in Registrar Lock Status unless the Registrant is provided with the reasonable opportunity and ability to unlock the domain name prior to the Transfer Request.*
> *d. Domain name registration period time constraints other than during the first 60 days of initial registration.*
> *e. General payment defaults between Registrar and business partners / affiliates in cases where the Registrant for the domain in question has paid for the registration.*

GNSO Inter-Registrar Policy Working Group on Clarification of Reasons for Denial

On 9 April 2008, the GNSO Inter-Registrar Policy Working Group on Clarification of Reasons for Denial reviewed the reasons for which a Losing Registrar may deny a registrant's request for an inter-registrar transfer and noted the language for four of the nine reasons was unclear. The Working Group noted the unclear language was causing varying interpretations and practices among registrars. The Working Group also explored possible ways to clarify the language.

Specifically, the Working Group on Clarification of Reasons for Denial noted the following four denial reasons as requiring additional clarification:

- Denial for nonpayment (reason 5)
- Denial for lock status (reason 7)
- Denial for 60 days of initial registration period (reason 8)
- Denial for 60 days after previous transfer (reason 9)

Following receipt of the Working Group's Final Report, the GNSO Council launched a drafting group to develop suggested text modifications for Reasons 5, 7, 8 and 9 on 17 April 2008.

The Drafting Team ultimately recommended the following changes to denial reasons 8 and 9:

Reason 8 proposed updated text: The transfer was requested within 60 days of the creation date as shown in the registry Whois record for the domain name.

Reason 9 proposed updated text: A domain name is within 60 days (or a lesser period to be determined) after being transferred (apart from being transferred back to the original Registrar in cases where both Registrars so agree and/or where a decision in the dispute resolution process so directs). "Transferred" shall only mean that an inter-registrar transfer, or transfer to the Registrar of Record has occurred in accordance with the procedures of this policy.

GNSO IRTP WG Part B

The GNSO IRTP Part B PDP Working Group was tasked with five issues related to domain name hijacking, the urgent return of an improperly transferred name, and the lock status of domain names, including, et.al.:

(3) Whether, and if so, how best to clarify denial reason #7: A domain name was already in "lock status" provided that the Registrar provides a readily accessible and reasonable means for the Registered Name Holder to remove the lock status.

Following discussion of this issue, the Working Group ultimately provided the following recommendations with respect to a Losing Registrar's reason for NACKing an inter-registrar request:

Recommendation 6: [...] The WG recommends to modify denial reason #6 as follows: Express objection to the transfer by the authorized Transfer Contact. Objection could take the form of specific request (either by paper or electronic means) by the authorized Transfer Contact to deny a particular transfer request, or a general objection to all transfer requests received by the Registrar, either temporarily or

indefinitely. In all cases, the objection must be provided with the express and informed consent of the authorized Transfer Contact on an opt-in basis and upon request by the authorized Transfer Contact, the Registrar must remove the lock or provide a reasonably accessible method for the authorized Transfer Contact to remove the lock within five (5) calendar days.

Recommendation 9: The WG recommends deleting denial reason #7 as a valid reason for denial under section 3 of the IRTP as it is technically not possible to initiate a transfer for a domain name that is locked, and hence cannot be denied, making this denial reason obsolete. Instead denial reason #7 should be replaced by adding a new provision in a different section of the IRTP on when and how domains may be locked or unlocked. [...]

3.1.6.3. Input Received in Response to the Policy Status Report

The World Intellectual Property Organization ("WIPO") provided a detailed comment around section 3.8.1 of the Transfer Policy, "3.8 The Registrar of Record must deny a transfer request in the following circumstances: 3.8.1 A pending UDRP proceeding that the Registrar has been informed of."

WIPO's public comment noted issues with the Transfer Policy's relationship with the UDRP, in particular domain (un)locking, UDRP decision implementation (i.e., case suspension and settlement), and cyberflight, which is a form of unauthorized domain transfer carried out during a pending UDRP case. WIPO posits that an ambiguity exists in the definition of a domain name "lock" and the responsibilities of gaining and losing registrars to "lock," or otherwise prevent transfer of, a domain name subject to a UDRP proceeding.

WIPO additionally notes that inter-registrar transfers of domain names subject to UDRP proceedings are still carried out, despite this being an explicit violation of the Transfer Policy. While the Losing Registrar holds the responsibility for NACKing an inter-registrar transfer request for domain names subject to a UDRP proceeding, the ambiguity associated with "locking" a domain name has resulted in many improper domain name transfers. WIPO's public comment noted the following issues with the Transfer Policy:

- A gaining registrar may not be on notice that a domain is subject to a UDRP proceeding, which results in that registrar accepting the transfer and being (unknowingly) in violation of the Transfer Policy.
- In some cases, registrars obligated to transfer a domain name to a complainant following a UDRP decision disclaim responsibility for that obligation, claiming they are only obliged to unlock the domain.
- In some instances inter-registrar transfers are rejected due to those transfers being requested within 60 days of the creation date or last transfer date.
- As it relates to cyberflight, incidences [reported to WIPO] have decreased, but still occur occasionally. The public comment notes the lack of a mechanism for dispute resolution providers to enforce registrar responsibilities as they relate to transferring a domain name back to the original registrar or registrant. Thus, despite a UDRP decision in favor of a complainant, sometimes domain names are still not returned to the original registrar and/or registrant.

WIPO recommended "that ICANN establish a standardized process for indicating that a domain is 'locked' due to a pending UDRP case (e.g., using an EPP code) and for communications between losing and gaining registrars to confirm a domain's status as it relates to UDRP proceedings before initiating a

transfer. WIPO's recommendations as they relate to the above involve developing clearer processes, instructions, and standards for:

- Enforcing the obligations of gaining and losing registrars to (not) transfer a domain as a result of a UDRP proceeding (e.g. by clarifying domain name "lock" status in the context of inter-registrar transfers);
- Communications between gaining and losing registrars regarding transfer requests for domains that may be subject to a UDRP proceeding;
- Engagement between dispute resolution providers and registrars to enforce a provider's decision requiring transfer of a domain name back to a complainant and/or original registrar.

3.1.6.4. Available Metrics Related to Denial of Transfers

The Transfer Policy Status Report, on p. 23, provides a chart showing the amount of NACK-ed transfers from the period of October 2009 - April 2018. With the exception of two spikes in the period, less than five percent of inter-registrar transfer requests are NACK-ed by the losing registrar. There was a spike in NACK-ed transfers in June 2012, and although the reason for the spike is not certain, it may correlate to the policy updates that went into effect as a result of the IRTP Working Group Part B's policy recommendations.

The Compliance data in the Transfer Policy Status Report contains a field showing "transfer[s] [that] cannot be completed because there is a pending Uniform Domain Name Dispute Resolution Policy (UDRP) action" (see PSR Section 3.1, Table 6, p. 35: "Transfer Related Complaints by Closure Code, 2012 – 2018"). The data shows that since 2012, Compliance has received two complaints regarding a transfer that could not be carried out due to a pending UDRP case.

When compiling data for the Transfer Policy Status Report, the authors conducted internal outreach to ICANN's Contractual Compliance Team. The Contractual Compliance Team observed the following with respect to NACK-ing of inter-registrar transfer requests: "[Clarification] of the wording in Section I.A.3.7.3 of the Transfer Policy about denial based upon payment for previous or current registration period [should be considered]. Registrars and reporters are confused by the current language." Additionally, the Contractual Compliance Team observed that Section I.A.3.9.1 of the Transfer Policy may require clarification, as there may be confusion with the meaning of pending registration period within the text, "nonpayment for a pending or future registration period."

3.1.6.5. Further Policy Questions for Consideration

1. Are the current reasons for denying or NACK-ing a transfer sufficiently clear? Should additional reasons be considered? For instance, ICANN Contractual Compliance has observed difficulties from registrars tying transfer denials involving domain names suspended for abusive activities to the denial instances contemplated by the Transfer Policy; or should any reasons be removed?
2. Should additional guidance around cases subject to a UDRP decision be provided to ensure consistent treatment by all registrars? If so, is this something that should be considered by the RPMs PDP Working Group's review of the UDRP, or should it be conducted within a Transfer Policy PDP?

3.1.7. ICANN-Approved Transfers

3.1.7.1. Background of ICANN-Approved Transfers

Section I.B of the Transfer Policy provides requirements related to an ICANN-approved bulk transfer of a registrar's gTLD domain names, or a portion thereof, to another registrar.

Specifically, Section I.B of the Transfer Policy provides:

> *1. Transfer of the sponsorship of all the registrations sponsored by one Registrar as the result of (i) acquisition of that Registrar or its assets by another Registrar, or (ii) lack of accreditation of that Registrar or lack of its authorization with the Registry Operator, may be made according to the following procedure:*
>
> *1.1 The gaining Registrar must be accredited by ICANN for the Registry TLD and must have in effect a Registry-Registrar Agreement with Registry Operator for the Registry TLD.*
>
> *1.2 ICANN must certify in writing to Registry Operator that the transfer would promote the community interest, such as the interest in stability that may be threatened by the actual or imminent business failure of a Registrar.*
>
> *2. Upon satisfaction of these two conditions, Registry Operator will make the necessary one-time changes in the Registry database for no charge, for transfers involving 50,000 name registrations or fewer. If the transfer involves registrations of more than 50,000 names, Registry Operator will charge the gaining Registrar a one-time flat fee of US$ 50,000.*

In short, if a registrar (i) is acquired by another ICANN-accredited registrar, (ii) voluntarily terminates its Registrar Accreditation Agreement (RAA) or allows expiration of the agreement without renewal, (iii) has its RAA terminated by ICANN, or (iv) has its Registry-Registrar Agreement (RRA) terminated by a registry operator, the registrar's domain names will need to be transferred to another ICANN-accredited registrar.

The bulk transfer provision (Part I.B) of the Transfer Policy is most often invoked in instances where a registrar's RAA is terminated or expires without renewal. Part I.B of the Transfer Policy also allows for bulk transfers in cases where a registrar lacks authorization to continue management of domains within a registry, such as when its RRA is terminated. In both cases, ICANN follows the De-Accredited Registrar Transition Procedure to identify an ICANN-accredited registrar to take over management of the names and notifies affected registries when it has approved the bulk transfer.

De-Accredited Registrar Transition Procedure

In consultation with the ICANN Community,[29] ICANN org developed the De-Accredited Registrar Transition Procedure, which is intended to provide a rapid, objective, and predictable procedure for transitioning domain names from a de-accredited registrar to an ICANN-accredited registrar. This procedure was developed to help protect registrants by ensuring their domain names are safely transferred to an ICANN-accredited registrar in the event of the termination (involuntary or voluntary) or non-renewal of their registrar.

Section 3 of the De-Accredited Registrar Transition Procedure provides:

> *"When a registrar's RRA or RRA is terminated or not renewed, it may often be in the best interests of registrants and at-large users of the Internet for ICANN to permit the de-accredited registrar to designate a 'gaining registrar' to receive a bulk transfer of its names. Such a transition could help minimize customer confusion while ensuring the gaining registrar receives as much customer and registration data from the losing registrar as possible. Moreover, a voluntary transition generally involves the least amount of friction in the process."*

ICANN org, through its use of the De-Accredited Registrar Transition Procedure, employs a balancing of interests to approve a proposed voluntary bulk transfer. The considerations in this decision include, without limitation: whether the gaining registrar is in good standing with its ICANN obligations, whether the gaining registrar is operational and experienced in managing the affected TLDs, whether there is a relationship between the losing registrar and gaining registrar that could allow abuse or gaming of the proposed bulk transfer, whether the losing registrar would continue to manage the registrations as a reseller for the gaining registrar or otherwise be involved in the management of the names and customers, and whether, as a result of the bulk transfer, obligations to ICANN and the losing registrar's customers are likely to be satisfied.

In instances where the de-accredited registrar does not nominate a proposed gaining registrar for its domain names or ICANN does not approve the proposed gaining registrar, ICANN uses the De-Accredited Registrar Transition Procedure to select a gaining registrar to manage the orphaned registrations. The gaining registrar selection process is described in more detail in Sections 6-9 of the De-Accredited Registrar Transition Procedure.

3.1.7.2 Additional Input

ICANN Org

In preparing this report, ICANN org Policy staff consulted with other departments within ICANN org. Colleagues from Global Domains and Strategy (GDS), who manage the De-Accredited Registrar Transition Procedure, have noted that the requirements in Section I.B.2 of the Transfer Policy have caused challenges in certain instances of de-accreditation. Specifically, the requirement for a gaining registrar to pay a one-time flat fee of $50,000 can make it difficult to secure a gaining registrar. By way of example, when the pool of potential gaining registrars perceive the value of a domain portfolio to be minimal, where the terminating registrar's domains are known or suspected to have a significant portion of abusive registrations, data escrow issues (the data in escrow is outdated or incomplete), or

[29] ICANN org held a session at ICANN31 in Delhi, India, where ICANN presented a proposal for the De-Accredited Transition Procedure. ICANN org also held a session ICANN45 in Toronto, Canada, where it discussed updates the De-Accredited Registrar Transition Procedure with the ICANN community.

expectations of renewal rates are low (in the case of aggressive promotions), the requirement for a gaining registrar to pay a one-time flat fee of $50,000 USD to the registry operator makes it difficult to secure a gaining registrar to accept the domains. This, in turn, poses a risk to the registrants who have utilized the services of the terminating registrar. Furthermore, ICANN has limited ability to determine the quality of the domains or make representations to potential gaining registrars as to the value of the domains.

Public Comment on Preliminary Issue Report

Three organizations participated in the public comment opportunity on the Preliminary Issue Report, and all three commenters recommended the topic of ICANN-approved transfers be further examined by the eventual working group. Specifically, commenters noted that the current scope of ICANN-approved bulk transfers is very limited, and an eventual working group should explore an updated policy that could accommodate bulk transfers not tied to an acquisition. One commenter noted, "although some registry operators utilize Bulk Transfer After Partial Portfolio Acquisition (BTAPPA), in order to provide this service, registry operators must first add it as an additional registry service through the Registry Services Evaluation Policy (RSEP). Because of these complicating factors, there may be differences between registry operators for bulk transfers, and not all registry operators may offer bulk transfers. The standardization of the bulk transfer process between registrars would allow registrars who are also acting as resellers to more efficiently consolidate their domains under management onto a single IANA credential, should they so desire. It may also harmonize divergent processes between registries, adding transparency and efficiency to the DNS ecosystem limits competition and free trade."

Taking the above comments into consideration, ICANN org has added an additional policy question for consideration.

3.1.7.3. Further Policy Questions for Consideration

1. In light of these challenges described in section 3.1.7.2 of the Final Issue Report, should the required fee in Section I.B.2 of the Transfer Policy be revisited or removed in certain circumstances?
2. Should the scope of voluntary bulk transfers, including partial bulk transfers, be expanded and/or made uniform across all of ICANN's contracted parties? If so, what types of policy considerations should govern voluntary bulk transfers and partial bulk transfers?

3.1.8. EPDP Phase 1, Recommendation 27 Wave 1 Report

3.1.8.1. Background of EPDP Phase 1, Recommendation 27 Wave 1 Report

As part of the EPDP Team's Phase 1 Final Report, the EPDP Team recommended, in Recommendation 27:

> *The EPDP Team recommends that as part of the implementation of these policy recommendations, updates are made to the following existing policies / procedures, and any others that may have been omitted, to ensure consistency with these policy recommendations as, for example, a number of these refer to administrative and/or technical contact which will no longer be required data elements:*
>
> - *Registry Registration Data Directory Services Consistent Labeling and Display Policy*
> - *Thick WHOIS Transition Policy for .COM, .NET, .JOBS*
> - *Rules for Uniform Domain Name Dispute Resolution Policy*
> - *WHOIS Data Reminder Policy*
> - *Transfer Policy*
> - *Uniform Rapid Suspension System (URS) Rules*
> - *Transfer Dispute Resolution Policy*

Following the Board's adoption of the EPDP Team's Final Report, ICANN org performed a detailed analysis of each existing consensus policy and procedure and how it may be impacted by the EPDP Team's policy recommendations. Following the review, ICANN org produced a report, which it shared with the Phase 1 Implementation Review Team and the GNSO Council for its consideration.

While the report includes an analysis of 15 policies and procedures, only two of the policies are relevant to this Final Issues Report. Specifically, the Recommendation 27 Wave 1 Report provides (i) an analysis of the impacted areas of the Transfer Policy and Transfer Dispute Resolution Policy, and (ii) potential changes to address the identified impacts of these policies. The identified impacts include, for example, outdated provision language (e.g., references to administrative contact requirements), higher-level issues such as the relevance or inconsistency of an existing policy or procedure with the new gTLD Registration Data Policy, or implications for existing contractual provisions. The estimated impact for both the Transfer Policy and the Transfer Dispute Resolution Policy is high.

3.1.8.2. ICANN org Recommendation 27, Wave 1 Analysis

ICANN Org's analysis on the Transfer Policy and Transfer Dispute Resolution Policy is excerpted below for ease of reference:

Transfer Policy

1. Section I.A.1.1 provides that either the Registrant or the Administrative Contact can approve or deny a transfer request. Under the Registration Data Policy, Administrative Contact data is no longer collected by the registrar. Accordingly, the registrant would be the only authorized transfer contact.

2. Section I.A 2.1, Gaining Registrar Requirements, relies on the specification of transfer authorities in section 1.1, defining either the Registrant and Administrative Contact as a "Transfer Contact." Given that

Administrative Contact data is no longer collected by the registrar, there may not be a need for “transfer contact” terminology, but such references can be replaced by “registrant” as the registrant is the only valid transfer authority. “Transfer Contact” terminology is referenced in part I (A) of the policy in sections 2.1, 2.1.1, 2.1.2, 2.1.2.1, 2.1.3.1(b), 2.1.3.3, 2.2.1, 3.2, 3.3, 3.6, 3.7.4, and 4.1.

3. Section I.A.3 enumerates the reasons a registrar of record may deny a transfer. These include paragraph 3.7.2, “reasonable dispute over the identity of the Registered Name Holder or Administrative Contact.” The Administrative Contact reference may be eliminated as the Administrative Contact data is no longer collected by the registrar. Paragraph I.A.3 also enumerates the reasons a registrar of record may not use to deny a transfer request. These include paragraph 3.9.2, “no response from the Registered Name Holder or Administrative Contact.” The Administrative Contact reference may be eliminated as the Administrative Contact data is no longer collected by the registrar.

4. Section I.A.4.6.5 provides that both registrars will retain correspondence in written or electronic form of any Transfer Emergency Action Contact (TEAC) communication and responses, and share copies of this documentation with ICANN and the registry operator upon request. This requirement does not appear to be affected by the new Registration Data Policy, which provides for retention of data elements for a period of 18 months following the life of the registration.

5. Section I.A.5.6 provides that the "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the Forms of Authorization (FOAs) still need to be used for authorization or confirmation of a transfer request, as described in Sections I.A.2, I.A.3, and I.A.4 of the policy. Where registrant contact data is not published, and absent an available mechanism for the Gaining Registrar to obtain such contact data, it is not feasible for a Gaining Registrar to send an FOA to the registrant contact data associated with an existing registration, as required by the policy. However, the requirement for the Registrar of Record to send an FOA confirming a transfer request (covered in section I.A.3) is still achievable as the registrar does not need to rely on publicly available data.

6. Section II.B.1, Availability of Change of Registrant, provides that “Registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely.” This language may be updated to clarify what updating registration data means, i.e., whether requirements differ according to whether a change of registrant changes anything that is displayed.

7. Section II.B.1.1.4 references the Administrative Contact. The context of this provision is to define a change of registrant as a material change to certain fields, including “Administrative Contact email address, if there is no Prior Registrant email address.” This section may no longer be necessary, as, under the new Registration Data Policy, Administrative Contact data is no longer collected by the registrar.

8. The Transfer Policy contains references to Whois in sections I.A.1.1, I.A.2.1.2, I.A.2.2.1, I.A.3.6, I.A.3.7.5, I.B.1, and the Notes section titled “Secure Mechanism.” If updates are considered to this policy as a result of GNSO policy work, it may be beneficial to consider replacing these references with RDDS. (The Temporary Specification, Appendix G, Section 2.2.4, on Supplemental Procedures to the Transfer Policy, provides that the term "Whois" SHALL have the same meaning as "RDDS.” This is carried over in the EPDP Phase 1 recommendation 24) Transfer Policy section II.C.1.4 provides that a registrar must obtain confirmation of a Change of Registrant request from the Prior Registrant, or the Designated Agent of such, using a secure mechanism to confirm that the Prior Registrant and/or their respective Designated Agents have explicitly consented to the Change of Registrant. The footnote to this section

notes that "The registrar may use additional contact information on file when obtaining confirmation from the Prior Registrant and is not limited to the publicly accessible Whois." If changes are considered to this policy as a result of GNSO policy work, it may be beneficial to consider updating this footnote to eliminate the reference to Whois.

9. The EPDP Team's Phase 1 Recommendation 24 recommends that the following requirements apply to the Transfer Policy until superseded by recommendations from the Transfer Policy review being undertaken by the GNSO Council:

> *(a) Until 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:*
>
> *(a1) The Gaining Registrar is not REQUIRED to obtain a Form of Authorization from the Transfer Contact.*
>
> *(a2) The Registrant MUST independently re-enter Registration Data with the Gaining Registrar. In such instance, the Gaining Registrar is not REQUIRED to follow the Change of Registrant Process as provided in Section II.C. of the Transfer Policy.*
>
> *(b) As used in the Transfer Policy:*
>
> *(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".*
>
> *(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".*
>
> *(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".*
>
> *(b4) The term "Whois" SHALL have the same meaning as "RDDS".*
>
> *(c) Registrar and Registry Operator SHALL follow best practices in generating and updating the"AuthInfo" code to facilitate a secure transfer process.*
>
> *(d) Registry Operator MUST verify that the "AuthInfo" code provided by the Gaining Registrar is valid in order to accept an inter-registrar transfer request. These requirements are being implemented as part of implementing the Registration Data Policy.*

10. Feedback from some stakeholders in June 2019 during an ICANN65 session suggested an approach of starting from a clean slate rather than looking at specific transfer issues individually. This appears to be the path the GNSO is taking, based on discussions at the September Council meeting.

Cross-reference: Section I.B.3.1 contains a footnote referencing the Expired Registration Recovery Policy. The context for this reference is a provision specifying when the Change of Registrant Procedure does not apply, in this case, when the registration agreement expires. The footnote provides that if registration and Whois details are changed following expiration of the domain name pursuant to the terms of the registration agreement, the protections of the Expired Registration Recovery Policy still apply.

Cross-reference: Section I.B.3.5 references the Expired Domain Deletion Policy. The context for this reference is a provision specifying when the Change of Registrant Procedure does not apply, in this case, when the Registrar updates the Prior Registrant's information in accordance with the Expired Domain Deletion Policy.

Gaining FOA

The Gaining FOA can be updated with language changes but the text is not substantively impacted by the Registration Data Policy. The policy requirements around use of this form are discussed in section 3.11 above.

The Gaining FOA includes instruction to "<insert Registered Name Holder or Administrative Contact of Record as listed in the WHOIS>" as well as text stating that: "You have received this message because you are listed as the Registered Name Holder or Administrative contact for this domain name in the WHOIS database." To the extent this form is retained, the language may be updated to eliminate "Administrative Contact" and "WHOIS" references.

Losing FOA

The Losing FOA can be updated with language changes but the text is not substantively impacted by the Registration Data Policy.

The sample form includes instruction to "<insert Registered Name Holder or Administrative Contact of Record as listed in the WHOIS>" as well as noting that "a registrar may choose to include one or more of the following in the message sent to the Registered Name Holder or Admin contact." To the extent this form is retained, the language may be updated to eliminate "Administrative Contact" and "WHOIS" references.

Transfer Dispute Resolution Policy

1. Section 2.2, Statute of Limitations, provides that a dispute must be filed within 12 months of the alleged violation. This is the stated basis for the EPDP Team's Phase 1 recommendation 15 requiring registrars to retain only those data elements deemed necessary for the purposes of the TDRP, for a period of fifteen months following the life of the registration plus three months to implement the decision, as the TDRP has "the longest justified retention period of one year." Accordingly, this provision can be maintained under the Registration Data Policy.

2. Sections 3.1.2(ii), 3.2.1, and 3.5.2 specify complainant contact information to be included in the complaint, which may include personal data. Processing of personal data that is not registration data is expected to be covered in the data processing terms in EPDP recommendations 22 and 26.

3. Section 3.1.4 (i)(b) references a "copy of Whois output." The context for this provision is a listing of documentary evidence to be annexed to a complaint by the gaining registrar. This requirement may need to be further defined for clarity on what data the registrar must copy and include. Applying the definition of “Whois data” to have the same meaning as “Registration Data” as provided in EPDP recommendation 24, this would include all data elements that were collected by the registrar.

4. Section 3.1.4(ii)(c) enumerates the materials to be annexed to a complaint by the losing registrar. This provision specifies that the losing registrar is expected to provide a history of any Whois registration data changes made to the applicable registration. This requirement may need to be further defined as to what constitutes Whois modifications i.e., changes to public and/or non-public data elements. This provision may also need to be revised to clarify the scope of history available to the registrar, as it can only go as far back as data is retained. If the relevant data retention policy and uses of registration data including TDRP were disclosed to the data subject at the time of registration, this should cover such disclosure within the applicable period.

5. Section 3.2.4 provides that a panel appointed by a TDRP provider will “review all applicable documentation and compare registrant/contact data with that contained within the authoritative Whois database and reach a conclusion not later than thirty (30) days after receipt of Response.” This provision relies on comparison with the "authoritative Whois database," which does not have a clear analogue in the new Registration Data Policy.

   The purpose of this provision appears to be for the panel to validate the information provided to them by the registrars; however, it is not clear what source a panel would use as a basis for comparison with the registrar submissions under the new policy. The TDRP provides for the panel to match what the registrars provide with its own lookup; this does not seem to be possible unless a) the panel requests non-public data from the registrar in a similar manner as a UDRP provider, which would result in duplicative data or b) the complaint only includes publicly accessible data, and the panel is able to request and obtain the non-public data from the registrar. Registration data held by the registry operator is not referenced in this section except to note that in cases where the Registrar of Record's Whois is not accessible or invalid, the applicable Registry Operator's Whois should be used, except in the case of a thin Registry, in which case the dispute should be placed on hold. It may be necessary to establish what is authoritative and what sources the panel should use in considering a TDRP complaint.

   Alternatively, the provisions of this section could be restated at a higher level to define what the panel is being asked to do. The specific steps regarding comparison of various registration data sources may not be the basis for the panel’s determination; rather, the panel is asked to consider the facts and circumstances and evidence presented by the parties to the dispute to determine whether a violation of the Transfer Policy has occurred.

3.1.8.3. Further Policy Questions for Consideration

The Transfer Policy Review Scoping Team is largely supportive of the findings within the ICANN Org’s Recommendation 27, Wave 1 Report, and noted the identified issues should also be included in the scope of a future PDP.

1. How should the identified issues be addressed?

2. Can the FOA-related Transfer Policy issues (identified in paragraphs 5 and 9 of Wave 1 Report),[30] as well as the proposed updates to the Gaining and Losing FOAs, be discussed and reviewed during the review of FOAs?
3. Can the Change of Registrant-related issue (identified in paragraph 6[31] of the Wave 1 report) be discussed and reviewed during the review of the Change of Registrant Process?
4. Can the identified Transfer Policy Dispute Resolution Policy Issues (noted in TDRP questions 1-5 of the Wave 1 report) be discussed and reviewed during the review of the TDRP?
5. Are there any Transfer Policy or Transfer Dispute Resolution Policy issues that were not captured in the Recommendation 27 Wave 1 Report that need to be considered?
6. Should these issues, or a subset of these issues, be resolved urgently rather than waiting for the respective PDP Working Group?

3.2. Relevant Documentation and Reports

- Transfer Policy Status Report
- EPDP Phase 1 Recommendation 27 Impact Analysis
- GNSO Transfer Policy Review Scoping Team Initial Scoping Document

3.3. Potential issues to be considered in a PDP on the Transfer Policy

The potential issues to be considered in the PDP on the Transfer Policy have been discussed at length and in more specificity in Section 3.1; however, the issues are included in this section for ease of reference.

- Whether the Gaining Registrar Form of Authorization ("FOA") or Losing Registrar are necessary; if so, do they require changes or enhancements (Please see Section 3.1.1)

[30] Paragraph 5: Section I.A.5.6 provides that the "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the Forms of Authorization (FOAs) still need to be used for authorization or confirmation of a transfer request, as described in Sections I.A.2, I.A.3, and I.A.4 of the policy. Where registrant contact data is not published, and absent an available mechanism for the Gaining Registrar to obtain such contact data, it is not feasible for a Gaining Registrar to send an FOA to the registrant contact data associated with an existing registration, as required by the policy. However, the requirement for the Registrar of Record to send an FOA confirming a transfer request (covered in section I.A.3) is still achievable as the registrar does not need to rely on publicly available data. Paragraph 9: The EPDP Team's Phase 1 Recommendation 24 recommends that the following requirements apply to the Transfer Policy until superseded by recommendations from the Transfer Policy review being undertaken by the GNSO Council (redacted for brevity).

[31] Paragraph 6: Section II.B.1, Availability of Change of Registrant, provides that "Registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely." This language may be updated to clarify what updating registration data means, i.e., whether requirements differ according to whether a change of registrant changes anything that is displayed.

- Whether changes should be considered to the management of AuthInfo Codes (Please see Section 3.1.2)
- Whether changes should be considered to the Change of Registrant process (Please see Section 3.1.3)
- Whether changes should be considered to the Transfer Emergency Action Contact ("TEAC") (Please see Section 3.1.4)
- Whether changes should be considered to the Transfer Dispute Resolution Policy (Please see Section 3.1.5)
- Whether changes should be considered to reasons for denial of inter-registrar transfers (Section 3.1.6)
- Whether changes should be considered to ICANN-approved inter-registrar bulk transfers (Section 3.1.7.)
- Whether updates to the Transfer Policy are required as a result of the Rec. 27, Wave 1 Report (Section 3.1.8)

3.4. Objectives of a possible PDP

A potential Transfer Policy Development Process would, at a minimum, (1) review and revise sections of the Transfer Policy that are no longer workable due to changes in data protection law, (2) review changes to the Transfer Policy as a result of IRTP Working Groups B, C, and D to determine if the policy recommendations resulted in their desired effects, and (3) review the security of inter-registrar and inter-registrant transfers and determine if updates are necessary.

The outcomes of a potential Transfer Policy PDP Working Group may include:

3.2.1.1. If a policy development process is initiated on the issues discussed in this report, the probable outcome would be the presentation to the GNSO Council of policy recommendations, which would detail modifications to the existing Transfer Policy. If the GNSO Council and the ICANN Board of Directors adopted the policy recommendations, this would result in the revised Transfer Policy being posted and notice provided to all Contracted Parties.

3.2.1.2. If a policy development process is not initiated, or if there are no changes recommended at the conclusion of a PDP, the result would be that the status quo would continue.

3.2.1.3. The presumption is that a PDP in accordance with the issues addressed in this report should not result in additional changes to the Transfer Policy beyond the specific areas discussed in this Report, as the scope of the PDP would be limited to the issues discussed in Section 3.1. If the PDP WG were to identify additional policy issues in the course of its work, the WG would have the ability to flag these issues to the GNSO Council. The GNSO Council could then determine whether or not to add the additional issues to the WG's charter.

3.5. Questions and issues to be analyzed in a possible PDP

The issues provided by the Transfer Policy Review Scoping Team and potential questions to consider based on Staff's research into the issues is also provided in Section 3.1 of the Report but has also been included in this section for reference.

Gaining Registrar FOA and Losing Registrar FOA (Inter-Registrar Transfers)

Gaining FOA

- Now that the updates based on IRTP B, IRTP C, and IRTP D have been in place for a few years and the ICANN Community has seen it in practice, what evidence or facts was the Working Group able to identify that shows the Gaining FOA is still needed, or is no longer necessary? (If the Working Group determines the answer to this question is yes, the Working Group will proceed to Questions 2 and 3. If the Working Group determines the answer to this question is no, the Working Group should proceed to Questions 4 and 5.)
- If the Working Group determines the answer to Question 1 is yes, 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)?
- 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?
- If not, does the AuthInfo 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.?
- Additionally, does the transmission of the AuthInfo Code provide for a sufficient "paper trail" for auditing and compliance purposes?

Additional Security Measures

- 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?

Losing FOA

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

AuthInfo Code Management (Inter-Registrar Transfers)

Auth-Info Codes Details

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

Bulk Use of Auth-Info Codes

- Should the ability for registrants to request AuthInfo Codes in bulk be streamlined and codified? If so, should additional security measures be considered?
- Does the CPH TechOps research provide a logical starting point for future policy work on AuthInfo Codes, or should other options be considered? 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?

Change of Registrant (Inter-Registrant Transfers)

Change of Registrant - Overall Policy

- 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?

- 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?
- 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.

60-Day Lock

- 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?
- 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?
- 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?
- 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?

- 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 ~~Registered Name Holder~~ **Prior Registrant** to opt out of the 60-day inter-registrar transfer lock prior to any Change of Registrant request."?

Change of Registrant - Privacy/Proxy Customers

- 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.[32] Are there additional scenarios that need to be considered that are not included in this list?
- 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?
- Are notifications provided to privacy/proxy customers regarding COR and changes to the privacy/proxy service information sufficient? For example, should 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?

[32] 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

Designated Agent

- 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?
- If the Designated Agent function is not operating as intended, should it be retained and modified? Eliminated?
- Are there alternative means to meet the objectives of Designated Agent role?
- 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?
- 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

- 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?

Transfer Emergency Action Contact (Inter-Registrar Transfers)

- Is additional data needed to support evaluation of the effectiveness of the TEAC mechanism? If so, what data is needed?
- The time frame (4 hours) for registrars to respond to communications via the TEAC channel has been raised as a concern by the Transfer Policy Review Scoping Team and in survey responses. Some have expressed that registries must, in practice, have 24x7 coverage by staff members with the appropriate competency to meet this requirement and the language skills to respond to communications from around the world. Is there merit to concerns that the requirement disproportionately impacts certain registrars, namely:
    a. Registrars located in regions outside of the Americas and Europe, because of significant time zone differences?
    b. Small and medium-sized registrars, which may not have a sufficiently large team to have 24x7 staff coverage with the necessary competency?
    c. Registrars in countries where English is not the primary language, who may, in practice, need to have English-speaking TEAC contacts to respond to requests in English?

To what extent should the 4-hour time frame be revisited in light of these concerns? Are there alternative means to address the underlying concerns other than adjusting the time frame?

- Section I.A.4.6.2 of the Transfer Policy states that "Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain." The Transfer Policy Review Scoping Team noted that this timeframe should be more clearly defined. Is additional guidance needed to define a "reasonable period of time" after which registrars should be expected to use a standard dispute resolution process?
- According to section I.A.4.6.2 of the Transfer Policy, the TEAC may be designated as a telephone number, and therefore some TEAC communications may take place by phone. The Transfer Policy Review Scoping Team flagged this provision as a potential item for further consideration. Do telephone communications provide a sufficient "paper trail" for registrars who may later wish to request a transfer "undo" based on failure by a TEAC to respond? Such a request would require the registrar to provide evidence that a phone call was made and not answered, or a call back was not received within 4 hours. Noting this requirement, should the option to communicate by phone be eliminated? Is an authoritative "system of record" for TEAC communications warranted? If so, what are the requirements for such a system?
- The Transfer Policy Review Scoping Team indicated that there are several factors that make a Registry Operator's obligation to "undo" a transfer under Section 6.4 of the Transfer Policy challenging:
    a. Registry Operators do not have access to the designated TEACs for each Registrar, making validation of an undo request nearly impossible.
    b. There is no way for Registry Operators to independently verify that a Registrar did not respond within the required time frame or at all since Registry Operators are not a party to, or copied on, communications between the Registrar TEACs.
    c. Transfer "undo" requests associated with the failure of a TEAC to respond are unilateral so there is no validation required prior to a Registry Operator taking action. This has, on occasion, led to a "he said", "she said" scenario.
    d. Follow on to 4.c., if the policy were to be updated to allow for some level of validation by the Registry Operator prior to taking action, the requirement to "undo" a transfer within 5 calendar days of receiving an TEAC undo request leaves little to no time to attempt to validate the request prior to taking the action.

To what extent are changes to the policy needed to address these concerns? Are there other pain points for Registry Operators that need to be considered in the review of the policy in this regard?

Transfer Dispute Resolution Policy (Inter-Registrar Transfers)

- Is there enough information available to determine if the TDRP is an effective mechanism for resolving disputes between registrars in cases of alleged violations of the IRTP? If not, what additional information is needed to make this determination?

- The ADNDRC reported to the IRTP Part D Working Group that in some of the cases it processed, appellees and appellants failed to provide sufficient information to support arbitration. Is this an issue that needs to be examined further in the context of the policy?
  a. Are the existing informational materials about the TDRP sufficient to ensure that registrars understand the process and the requirements for filing a dispute, including the information they need to give to the dispute resolution provider?
- If the TDRP is considered to be insufficient:
  a. Are additional mechanisms needed to supplement the TDRP?
  b. Should the approach to the TDRP itself be reconsidered?
- Are requirements for the processing of registration data, as specified in the TDRP, compliant with data protection law?
- Are requirements for the processing of registration data, as specified in the TDRP, appropriate based on principles of privacy by design and data processing minimization?

Denying Transfers (Inter-Registrar Transfers)

- Are the current reasons for denying or NACK-ing a transfer sufficiently clear? Should additional reasons be considered? For instance, ICANN Contractual Compliance has observed difficulties from registrars tying transfer denials involving domain names suspended for abusive activities to the denial instances contemplated by the Transfer Policy; or should any reasons be removed?
- Should additional guidance around cases subject to a UDRP decision be provided to ensure consistent treatment by all registrars? If so, is this something that should be considered by the RPMs PDP Working Group's review of the UDRP, or should it be conducted within a Transfer Policy PDP?

ICANN-approved Transfers

- In light of challenges described within this report, should the required fee in Section I.B.2 of the Transfer Policy be revisited or removed in certain circumstances?
- Should the scope of voluntary bulk transfers, including partial bulk transfers, be expanded and/or made uniform across all of ICANN's contracted parties? If so, what types policy considerations should govern voluntary bulk transfers and partial bulk transfers?

Wave 1, Recommendation 27 Report (Inter-Registrar and Inter-Registrant Transfers)

- How should the identified issues be addressed?
- Can the FOA-related Transfer Policy issues (identified in paragraphs 5 and 9 of Wave 1 Report),[33] as well as the proposed updates to the Gaining and Losing FOAs, be discussed and reviewed during the review of FOAs?

[33] Paragraph 5: Section I.A.5.6 provides that the "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the Forms of Authorization (FOAs) still need to be used for authorization or confirmation of a transfer request, as described in Sections I.A.2, I.A.3, and I.A.4 of the policy. Where registrant contact data is not published, and absent an available mechanism for the Gaining Registrar to obtain such contact data, it is not feasible for a Gaining Registrar to send an FOA to the

- Can the Change of Registrant-related issue (identified in paragraph 6[34] of the Wave 1 report) be discussed and reviewed during the review of the Change of Registrant Process?
- Can the identified Transfer Policy Dispute Resolution Policy Issues (noted in TDRP questions 1-5 of the Wave 1 report) be discussed and reviewed during the review of the TDRP?
- Are there any Transfer Policy or Transfer Dispute Resolution Policy issues that were not captured in the Recommendation 27 Wave 1 Report that need to be considered?
- Should these issues, or a subset of these issues, be resolved urgently rather than waiting for the respective PDP Working Group?

3.6. Other factors relevant to the decision whether to initiate a PDP

- **Effect of recent privacy laws on efficacy and workability of the Transfer Policy**: The Transfer Policy Review Scoping Team noted the GDPR and similar national privacy legislation have rendered the certain parts of Transfer Policy ineffective and unworkable as written. For example, and as noted in Section 3.1.1 of this Report, the Gaining Registrar may be unable to send the Gaining FOA due to its inability to obtain current registration data via the public Registration Data Directory Services ("RDDS"). This is because the Registrar of Record (or Losing Registrar) may be required to redact certain registration data due to data protection law requirements. Accordingly, the ICANN Community would benefit from the development of a fully-functioning Policy.

- **Outstanding policy issues expected to be dealt with in an eventual Transfer Policy PDP**: There are two communications between the ICANN Board and GNSO Council wherein outstanding Transfer Policy issues are referenced: namely, (1) if the addition/removal of a privacy/proxy service constitutes a Change of Registrant under the Transfer Policy, and (2) Gaining FOA compliance enforcement. If these issues are not addressed in a Transfer Policy PDP, when and how would the Council recommend they be dealt with?

- **Resources available:** The GNSO Council will need to consider, taking into account the current workload and resources, whether there is sufficient bandwidth to take on this issue at this time, and whether other projects may need to be halted should it decide to move forward.

registrant contact data associated with an existing registration, as required by the policy. However, the requirement for the Registrar of Record to send an FOA confirming a transfer request (covered in section I.A.3) is still achievable as the registrar does not need to rely on publicly available data. Paragraph 9: The EPDP Team's Phase 1 Recommendation 24 recommends that the following requirements apply to the Transfer Policy until superseded by recommendations from the Transfer Policy review being undertaken by the GNSO Council (redacted for brevity).

[34] Paragraph 6: Section II.B.1, Availability of Change of Registrant, provides that "Registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely." This language may be updated to clarify what updating registration data means, i.e., whether requirements differ according to whether a change of registrant changes anything that is displayed.

4 Staff Recommendation

4.1. General Counsel recommendation

Based on the analysis below, the launch of a dedicated policy development process limited to consideration of the issues identified in this Report has been confirmed by the General Counsel to be properly within the scope of the ICANN policy process and within the scope of the GNSO.

4.2. Scope considerations

The launch of a dedicated Policy Development Process limited to consideration of the issues described in Section 3 of this report has been confirmed by the General Counsel to be properly within the scope of the ICANN policy process and within scope of the GNSO.

4.3. Whether the issue is within the scope of ICANN's mission statement

ICANN's mission statement includes the coordination of the allocation of certain types of unique identifiers, including domain names, and the coordination of policy development reasonably and appropriately related to these technical functions.

4.4. Whether the issue is broadly applicable to multiple situations or organizations

Inter-registrar transfers and inter-registrant transfers affect Contracted Parties (both Registries/Registrars), registrants, and rights holders.

Registries and Registrars are both required to comply with the Transfer Policy, as it is an approved ICANN Consensus Policy; accordingly, Contracted Parties are currently affected by the inoperable sections of the Transfer Policy (as a result of data protection law changes). Contracted Parties would also be affected by any changes to the Transfer Policy as they may have to update their systems and business procedures in order to comply with any new requirements.

The Transfer Policy is also directly applicable to all gTLD registrants (individuals and organizations), as the Transfer Policy governs registrants' ability to change their registrar, which allows for consumer choice and competition.

Lastly, the Transfer Policy also implicates rights holders, as the Transfer Policy imposes restrictions, et. al., on inter-registrar and inter-registrant transfers while a domain name is subject to a UDRP or URS dispute.

Other ICANN Supporting Organizations and Advisory Committees will also likely be interested in the issue and the outcomes of a PDP, given the potential impact of the Transfer Policy on Internet users and the general public.

4.5. Whether the issue is likely to have lasting value of applicability

Enhancements and changes to the existing Transfer Policy will have lasting value and applicability, as the Transfer Policy will continue to apply to gTLD registries and registrars.

4.6. Whether the issue implicates or affects ICANN Consensus Policy

Enhancements and changes to the Transfer Policy issues would directly implicate the Transfer Policy.

4.7. ICANN org recommendations

ICANN org has confirmed that the proposed issues are within the scope of the policy development process and the GNSO. It is reasonable from the org's perspective to expect that enhancements of the Transfer Policy would be beneficial to the community generally, particularly for registrants, as well as those parties (gTLD registries and registrars) who are obligated to comply with the policy provisions. ICANN org, therefore, recommends that the GNSO Council proceed with a multi-phased PDP limited to consideration of the issues discussed in this report.

In recognition of the PDP 3.0 Guidelines, Enhancement 11, which provides "a PDP should have a narrow scope and, in those cases where a subject is broad, it needs to be broken into manageable pieces," ICANN org is recommending a two-phased PDP on the Transfer Policy to assist in making the policy work more manageable and achievable. To that end, ICANN org is recommending the GNSO consider the following phasing and sequencing of the Transfer Policy PDP:

1. Phase 1(a): Form of Authorization (including Rec. 27, Wave 1 FOA issues) and AuthInfo Codes
2. Phase 1(b): Change of Registrant (including Rec. 27, Change of Registrant issues)
3. Phase 2: Transfer Emergency Action Contact and reversing inter-registrar transfers, TDRP (including Rec. 27, Wave 1 TDRP issues), NACKing transfers, ICANN-approved transfers

ICANN org recommends the two-phased PDP be included under the same charter, which would prevent the GNSO Council from having to initiate multiple PDPs and adopt multiple charters.

ICANN org recommends the work be conducted in two phases, as described above. More specifically, the two-phased PDP would entail the Working Group beginning its work on Phase 1(a) by working to produce an initial report based on the Phase 1(a) charter questions (FOA and AuthInfo Codes) and a second initial report based on the Phase 1(b) charter questions (Change of Registrant). The Working Group would then produce a final report for Phase 1, which include policy recommendations for Phase 1(a) and Phase 1(b). Following completion of the Phase 1 final report, the Working Group would send its

final report to the GNSO Council and Board, and, pending adoption by the ICANN Board, the Phase 1 policy recommendations would go into the implementation phase.

Following the Working Group's delivery of its Phase 1 final report to the GNSO Council, the Working Group would consult with the GNSO Council to see if any charter updates are necessary (for example, changes to Phase 2 based on the Working Groups experience in Phase 1). Following the consultation, the Working Group would take an agreed-upon break (example - 1 month) before commencing its work on the Phase 2 charter questions, while ICANN org works to implement the Phase 1 policy recommendations. During the break, Working Group members would have the opportunity to step down and allow new members to join.

In the event ICANN org or the Implementation Review Team identifies a dependency that affects Phase 2 of the Working Group's work plan, the issue would be communicated to the Working Group. The Working Group would then be tasked with considering the identified issue(s) during Phase 2 to enable a holistic review of the identified issue(s).

ICANN org is recommending Phase 1(a) consist of issues related to Form of Authorization and AuthInfo Codes due to the outstanding compliance enforcement issues discussed in Section 3.1.1.2 of this report. For this reason, ICANN org is recommending this issue be discussed more urgently than the others. The recommended phasing seeks to bundle related topics but does not preclude the Working Group from (i) bunding the topics differently or (ii) phasing the work differently (one phase instead of two phases).

5 Next Steps

In accordance with the GNSO PDP rules, ICANN org published the Preliminary Issue Report for public comment in order to allow for Community input on additional information, or the correction or updating of any information provided so far. Following review of the public comments, ICANN org updated the Preliminary Issue Report and will submit a summary of the comments received together with the Final Issue Report to the GNSO Council for its consideration. The GNSO Council will then vote on the staff recommendations, as to whether or not to go ahead and initiate a PDP on the Transfer Policy. It should be noted that the GNSO Council is not bound by Staff recommendations, and, if it chooses to do so, may pursue alternative actions to those proposed in this Final Issue Report.

Annex A Preliminary Charter

Please note the below is partially-completed Charter Template, in the event the GNSO Council chooses to launch a PDP on the Transfer Policy. This draft is not intended to presume a PDP will be launched, nor is it intended to bind the GNSO Council or Charter Drafting Team (if applicable) to specific language or formulations. Per Section 9 of the PDP Manual, "upon initiation of the PDP, the Council considers whether to adopt the proposed charter for the PDP WG as included in the Final Issue Report. If the Council decides not to adopt the proposed charter for the PDP WG as included in the Final Issue Group, a group formed at the direction of Council should be convened to draft the charter for the PDP Team or revise the proposed charter for the PDP WG as included in the Final Issue Report."

As a starting point, ICANN org has drafted this Charter Template based on the Transfer Policy Review Scoping Team's, and ICANN org's recommendation to group the Transfer Policy issues by topics, keeping in mind the PDP 3.0 recommendation that a PDP should have a narrow scope, and, in those cases where a subject is broad, it needs to be broken into manageable pieces. For purposes of the Final Issue report, ICANN org has focused on the following components of the draft Charter: (i) Mission and Scope; (ii) Deliverables; (iii) Data and Metrics Requirements; (iv) Working Group Model (v) Membership Requirements; and (vi) Membership Criteria.

Revised GNSO Working Group Charter Template

Version Date: 14 January 2020

ICANN | GNSO
Generic Names Supporting Organization

WG Name:	**TBD**
Section I: Working Group Identification	
Chartering Organization(s):	Generic Names Supporting Organization (GNSO) Council

Charter Approval Date:	<Enter Approval Date>	
Name of WG Leadership:	<Enter Elected WG Leadership)>	
Name(s) of Appointed Liaison(s):	<Enter Liaison>	
WG Workspace URL:	<Enter Active Project URL from GNSO Site>	
WG Mailing List:	<Enter Mailman archive link>	
GNSO Council Resolution:	**Title:**	<Enter Resolution Title>
	Ref # & Link:	<Enter Resolution link>
Important Document Links:	•	
Section II: Mission, Purpose, and Deliverables		
Mission & Scope:		

Background

At its meeting on DD MONTH YYYY, the GNSO Council unanimously adopted the initiation of a Working Group to deliberate the issues of topic X [.....TO BE COMPLETED……]

Mission and Scope

This Working Group (WG) is tasked to provide the GNSO Council with policy recommendations regarding whether to [.....TO BE COMPLETED……]

[Sample text provided by Staff]:

[The Working Group (WG) is tasked to provide the GNSO Council with policy recommendations on the Transfer Policy; specifically, the WG is to conduct a holistic review of the Transfer Policy and determine if changes to the policy are needed to improve the ease, security, and efficacy of inter-registrar and inter-registrant transfers. As part of this determination, the WG is, at a minimum, expected to consider the following elements of the Transfer Policy and answer the following charter questions during Phase 1 of its work.

Phase 1(a)

As part of its deliberations, the PDP WG should, at a minimum, consider the following issues detailed in the [INSERT LINK]. These are:

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

As a result, the WG should deliberate and consider the following Charter questions:

a) **Gaining Registrar FOA and Losing Registrar FOA**
a1) Now that the updates based on IRTP B, IRTP C, and IRTP D have been in place for a few years and the ICANN Community has seen it in practice, what evidence or facts was the Working Group able to identify that shows the Gaining FOA is still needed, or is no longer necessary? (If the Working Group determines the answer to this question is yes, the Working Group will proceed to Questions 2 and 3. If the Working Group determines the answer to this question is no, the Working Group should proceed to Questions 4 and 5.)

a2) If the Working Group determines the answer to Question 1 is yes, 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)?

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?

a4) If not, does the AuthInfo 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.?

a5) Additionally, does the transmission of the AuthInfo Code provide for a sufficient "paper trail" for auditing and compliance purposes?

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?

Losing FOA

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

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?

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?

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?

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?

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?

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.)?

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?

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

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?

c) **Wave 1, Rec. 27**

c1) How should the identified issues be addressed?

c2) Can the FOA-related Transfer Policy issues (identified in paragraphs 5 and 9 of Wave 1 Report),[35] as well as the proposed updates to the Gaining and Losing FOAs, be discussed and reviewed during the review of FOAs?

[Phase 1(b)

As part of its deliberations, the PDP WG should, at a minimum, consider the following issues detailed in the [Final Issue Report –INSERT LINK]. These are:

d) **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

35

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?

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?

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.

e) **60-Day Lock**

e1) 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?

e2) 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?

e3) 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?

e4) 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?

e5) 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."?

f) **Change of Registrant - Privacy/Proxy Customers**

f1) 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.[36] Are there additional scenarios that need to be considered that are not included in this list?

f2) 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?

f3) Are notifications provided to privacy/proxy customers regarding COR and changes to the privacy/proxy service information sufficient? For example, should 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?

g) **Designated Agent**

g1) 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?

g2) If the Designated Agent function is not operating as intended, should it be retained and modified? Eliminated?

g3) Are there alternative means to meet the objectives of Designated Agent role?

g4) 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?

g5) 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?

h) **Additional Questions**

h1) 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

[36] 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

requests, and should have the option accept or reject, over EPP notifications." Should this proposal be pursued further? Why or why not?

i) **Wave 1, Rec. 27**

i1) Can the FOA-related Transfer Policy issues (identified in paragraphs 5 and 9 of Wave 1 Report),[37] as well as the proposed updates to the Gaining and Losing FOAs, be discussed and reviewed during the review of FOAs?

[Phase 2

As part of its deliberations, the PDP WG should, at a minimum, consider the following issues detailed in the [Final Issue Report – INSERT LINK]. These are:

j) **Transfer Emergency Action Contact (Inter-Registrar Transfers)**

j1) Is additional data needed to support evaluation of the effectiveness of the TEAC mechanism? If so, what data is needed?

j2) The time frame (4 hours) for registrars to respond to communications via the TEAC channel has been raised as a concern by the Transfer Policy Review Scoping Team and in survey responses. Some have expressed that registries must, in practice, have 24x7 coverage by staff members with the appropriate competency to meet this requirement and the language skills to respond to communications from around the world. Is there merit to concerns that the requirement disproportionately impacts certain registrars, namely:

i. Registrars located in regions outside of the Americas and Europe, because of significant time zone differences?

ii. Small and medium-sized registrars, which may not have a sufficiently large team to have 24x7 staff coverage with the necessary competency?

[37] Paragraph 5: Section I.A.5.6 provides that the "AuthInfo" codes must be used solely to identify a Registered Name Holder, whereas the Forms of Authorization (FOAs) still need to be used for authorization or confirmation of a transfer request, as described in Sections I.A.2, I.A.3, and I.A.4 of the policy. Where registrant contact data is not published, and absent an available mechanism for the Gaining Registrar to obtain such contact data, it is not feasible for a Gaining Registrar to send an FOA to the registrant contact data associated with an existing registration, as required by the policy. However, the requirement for the Registrar of Record to send an FOA confirming a transfer request (covered in section I.A.3) is still achievable as the registrar does not need to rely on publicly available data. Paragraph 9: The EPDP Team's Phase 1 Recommendation 24 recommends that the following requirements apply to the Transfer Policy until superseded by recommendations from the Transfer Policy review being undertaken by the GNSO Council (redacted for brevity).

iii.Registrars in countries where English is not the primary language, who may, in practice, need to have English-speaking TEAC contacts to respond to requests in English?

To what extent should the 4 hour time frame be revisited in light of these concerns? Are there alternative means to address the underlying concerns other than adjusting the time frame?

j3) Section I.A.4.6.2 of the Transfer Policy states that "Communications to a TEAC must be initiated in a timely manner, within a reasonable period of time following the alleged unauthorized loss of a domain." The Transfer Policy Review Scoping Team noted that this timeframe should be more clearly defined. Is additional guidance needed to define a "reasonable period of time" after which registrars should be expected to use a standard dispute resolution process?

j4) According to section I.A.4.6.2 of the Transfer Policy, the TEAC may be designated as a telephone number, and therefore some TEAC communications may take place by phone. The Transfer Policy Review Scoping Team flagged this provision as a potential item for further consideration. Do telephone communications provide a sufficient "paper trail" for registrars who may later wish to request a transfer "undo" based on failure by a TEAC to respond? Such a request would require the registrar to provide evidence that a phone call was made and not answered, or a call back was not received within 4 hours. Noting this requirement, should the option to communicate by phone be eliminated? Is an authoritative "system of record" for TEAC communications warranted? If so, what are the requirements for such a system?

j5) The Transfer Policy Review Scoping Team indicated that there are several factors that make a Registry Operator's obligation to "undo" a transfer under Section 6.4 of the Transfer Policy challenging:

i. Registry Operators do not have access to the designated TEACs for each Registrar, making validation of an undo request nearly impossible.
ii. There is no way for Registry Operators to independently verify that a Registrar did not respond within the required time frame or at all since Registry Operators are not a party to, or copied on, communications between the Registrar TEACs.
iii. Transfer "undo" requests associated with the failure of a TEAC to respond are unilateral so there is no validation required prior to a Registry Operator taking action. This has, on occasion, led to a "he said", "she said" scenario.
iv. Follow on to 4.c., if the policy were to be updated to allow for some level of validation by the Registry Operator prior to taking action, the requirement to "undo" a transfer within 5 calendar days of receiving an TEAC undo request leaves little to no time to attempt to validate the request prior to taking the action.

To what extent are changes to the policy needed to address these concerns? Are there other pain points for Registry Operators that need to be considered in the review of the policy in this regard?

k) **Transfer Dispute Resolution Policy (Inter-Registrar Transfers)**

k1) Is there enough information available to determine if the TDRP is an effective mechanism for resolving disputes between registrars in cases of alleged violations of the IRTP? If not, what additional information is needed to make this determination?

k2) The ADNDRC reported to the IRTP Part D Working Group that in some of the cases it processed, appellees and appellants failed to provide sufficient information to support arbitration. Is this an issue that needs to be examined further in the context of the policy?

i. Are the existing informational materials about the TDRP sufficient to ensure that registrars understand the process and the requirements for filing a dispute, including the information they need to give to the dispute resolution provider?

k3) If the TDRP is considered to be insufficient:

i. Are additional mechanisms needed to supplement the TDRP?
ii. Should the approach to the TDRP itself be reconsidered?

k4) Are requirements for the processing of registration data, as specified in the TDRP, compliant with data protection law?

k5) Are requirements for the processing of registration data, as specified in the TDRP, appropriate based on principles of privacy by design and data processing minimization?

l) **Denying Transfers (Inter-Registrar Transfers)**

l1) Are the current reasons for denying or NACK-ing a transfer sufficiently clear? Should additional reasons be considered? For instance, ICANN Contractual Compliance has observed difficulties from registrars tying transfer denials involving domain names suspended for abusive activities to the denial instances contemplated by the Transfer Policy; or should any reasons be removed?

l2) Should additional guidance around cases subject to a UDRP decision be provided to ensure consistent treatment by all registrars? If so, is this something that should be considered by the RPMs PDP Working Group's review of the UDRP, or should it be conducted within a Transfer Policy PDP?

m) **ICANN-approved Transfers**

m1) In light of these challenges described in section 3.1.7.2 of the Final Issue Report, should the required fee in Section I.B.2 of the Transfer Policy be revisited or removed in certain circumstances?
m2) Should the scope of voluntary bulk transfers, including partial bulk transfers, be expanded and/or made uniform across all registry operators? If so, what types of rules and considerations should govern voluntary bulk transfers and partial bulk transfers?

n) **Wave 1, Recommendation 27 Report (Inter-Registrar and Inter-Registrant Transfers)**

n1) How should the identified issues be addressed?
n2) 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?

n3) Can the identified Transfer Policy Dispute Resolution Policy Issues (noted in TDRP questions 1-5 of the Wave 1 report) be discussed and reviewed during the review of the TDRP?
n4) Are there any Transfer Policy or Transfer Dispute Resolution Policy issues that were not captured in the Recommendation 27 Wave 1 Report that need to be considered?
n5) Should these issues, or a subset of these issues, be resolved urgently rather than waiting for the respective PDP Working Group?

Deliverables:

To develop, at a minimum, an Initial Report and a Final Report [for each of the phases] regarding the WG's recommendations on issues relating to the [.....TO BE COMPLETED……], following the processes described in Annex A of the ICANN Bylaws and the GNSO PDP Manual.

[If the WG concludes with any recommendations, the WG shall (or recommend the subsequent policy Implementation Review Team to) conduct a policy impact analysis and identify a set of metrics to measure the effectiveness of the policy change, including source(s) of baseline data for that purpose:

- **Identification of policy goals**

  [For example, the previous IRTP WGs reviewed and suggested improvements to the Transfer Policy based on the following underlying goals:
  - (1) Enabling registered name holders to move their domain names to a new provider, thereby increasing consumer choice and competition;
  - (2) Ensuring the IRTP includes sufficient protections to prevent fraudulent domain name transfers and domain name hijacking;
  - (3) Clarifying the language of the IRTP so that ICANN-accredited registrars consistently interpret and apply the policy;
  - (4) Clarifying the language and visibility of the Transfer Dispute Resolution Policy so that providers/panelists consistently interpret and apply the policy.

  Are these previously-identified policy goals an appropriate basis for the charter, or are new goals needed?]

- **Identification of metrics used to measure whether policy goals are achieved**

  <u>Phase 1(a)</u>
  [Based on the above-referenced policy goals, the following metrics may be helpful in identifying if a change to FOA or auth-code requirements has resulted in a change to the portability of domain names or the security of domain name transfers:
  - Number of inter-registrar transfers successfully completed, i.e., could less successful inter-registrar transfers indicate the policy changes have resulted in an unintended domain name portability issue?
  - Number of inter-registrar transfers denied/NACKed
  - Number of times the TEAC was contacted due to an improper transfer

- Number of ICANN Compliance complaints related to domain name hijacking (has there been an increase?)
- Number of ICANN Compliance complaints related to inability to retrieve AuthInfo Code
- Online survey to groups within the ICANN Community to gather input on the specific changes to the Transfer Policy - have the changes resulted in increased security? Are the changes being applied consistently by registrars and registries?]

Phase 1(b)

[Based on the above-referenced policy goals, the following metrics may be helpful in identifying if a change to the Change of Registrant process has resulted in a change to the portability of domain names or the prevention of fraudulent transfers:

- Number of Change of Registrants successfully completed, i.e., could a decrease in the number of Change of Registrants indicate the policy changes have resulted in an unintended domain name portability issue?
- Number of ICANN Compliance complaints related to domain name hijacking (has there been an increase?)
- Number of ICANN Compliance complaints related to the 60-day inter-registrar transfer lock?
- Online survey to groups within the ICANN Community to gather input on the specific changes to the Transfer Policy - have the changes resulted in increased security? Are the changes being applied consistently by registrars and registries?]

Phase 2

[Based on the above-referenced policy goals, the following metrics may be helpful in identifying if a change to the TEAC requirements has resulted in a change to the portability of domain names or the prevention of fraudulent transfers:

- Total number of TEAC requests
- Number of TEAC requests responded to within the required timeframe vs. number of TEAC requests NOT responded to within the required timeframe
- Number of TEAC requests resulting in a “transfer undo”
- Number of TEAC-related compliance complaints

[Based on the above-referenced policy goals, the following metrics may be helpful in identifying if a change to the TDRP requirements has resulted in increased visibility and consistent interpretation of the TDRP:

- Number of TDRP cases filed before and after changes (if any) go into effect
- Number of TDRP-related compliance complaints

[Based on the above-referenced policy goals, the following metrics may be helpful in identifying if a change to reasons for NACKing/denying transfers has resulted in a change to the portability of domain names or the prevention of fraudulent transfers:

- Number of successful inter-registrar transfers vs. number of inter-registrar transfers denied/NACKed
- Number of NACK-related compliance complaints
- Number of UDRP-NACKing related compliance complaints

[Based on the above-referenced policy goals, the following metrics may be helpful in identifying if updates (if any) to ICANN-approved transfers has resulted in a change to the portability of domain names and protection of registrants:

- Number of ICANN-approved bulk transfers
- Number of requested bulk transfers not approved by ICANN
- Number of complaints received by ICANN Compliance related to ICANN-approved bulk transfers

- **Identification of potential problems in attaining the data or developing the metrics**
  - Obtaining survey responses from registrants may prove difficult
- **A suggested timeframe in which the measures should be performed**
  - Approximately one year following the implementation of Transfer Policy changes
- **Define current state baselines of the policy and define initial benchmarks that define success or failure**
- **Metrics may include but not limited to (Refer to the Hints & Tips Page)**:
  - ICANN Compliance data
  - Industry metric sources
  - Community input via public comment
  - Surveys or studies]

Data and Metrics Requirements

The WG should as soon as practicable:

1. Determine a set of questions which, when answered, provide the insight necessary to achieve the policy goals.

[Policy goal of domain name portability:

(1) Have the recommended updates to the Transfer Policy (if any) resulted in a statistically significant change to the number of inter-registrar transfers? For example, if there is a statistically significant change to the number of requested inter-registrar transfers, the policy updates may have inhibited the underlying goals of domain name portability.

(2) Have changes to the FOAs (if any) resulted in a statistically significant increase in the number of (i) ICANN compliance complaints regarding improper transfers (ii) TEAC communications regarding improper transfers or (iii) TDRP filings?

Policy goal of ensuring the IRTP includes sufficient protections to prevent fraudulent domain name transfers and domain name hijacking:

(3) If security improvements are recommended to the AuthInfo Code, has there been a statistically significant decrease in the amount (i) ICANN compliance complaints regarding improper transfers (ii) TEAC communications regarding improper transfers or (iii) TDRP filings?

(4) If security improvements are recommended to the Change of Registrant process, (i) ICANN compliance complaints regarding improper transfers (ii) TEAC communications regarding improper transfers or (iii) TDRP filings?

(5) Have changes to TEAC requirements (if any) resulted in a statistically significant change to ICANN compliance complaints regarding improper transfers?

Policy goal of clarifying the language of the IRTP so that ICANN-accredited registrars consistently interpret and apply the policy:

(6) Is there data, via audits or Contractual Compliance complaints, showing that registrars have applied the updated policy language, implemented as a result of these policy recommendations, inconsistently?

Policy goal of clarifying the language and visibility of the Transfer Dispute Resolution Policy so that providers/panelists consistently interpret and apply the policy.

(7) If changes have been made to the TDRP, has there been a statistically significant change in the amount of (i) TDRP-related compliance inquiries or (ii) TDRP filings?]

2. Determine whether certain data is required to help understand a specific issue or answer a charter question.

[With respect to charter question a1, has there been a statistically significant increase in the number of contractual compliance complaints related to improper inter-registrar transfers following 25 May 2018, the effective date of the Temporary Specification (when the Gaining FOA requirement was eliminated in certain instances)?]

3. Determine a set of data and metrics which can be collected and analyzed to help answer the specific question.
4. Submit a Working Group Metrics Request Form (see GNSO Working Group Guidelines Section 4.5), if data gathering at the charter drafting phase or during the working phase is deemed necessary.

WG leaders shall review the Guidance document below to understand the need for performing due diligence before submitting a data gathering request to the GNSO Council.

Guidance: Checklist: Criteria to Evaluate Request for Data Gathering

Instruction for Charter Drafting Team
Please include the Working Group Metrics Request Form if data gathering during the chartering phase is required

Example: Request Form submitted by the GNSO Review of All Rights Protection Mechanisms in All gTLDs PDP Working Group

Section III: Project Management

Work Product Requirement:

The WG shall respect the timelines and deliverables as outlined in Annex A of the ICANN Bylaws and the PDP Manual. The WG leadership, in collaboration with the WG support staff and GNSO Council liaison, shall use a standard set of project management work products that help plan, guide, track, and report the progress of the WG from start to finish, and include the necessary data and information to assess the progress of the WG. These work products include:

- Summary Timeline
- Project Situation Report
- Project Plan
- Work Plan
- Action Items

Guidance: GNSO Project Work Product Catalog

Instruction for Charter Drafting Team
Please include any work products that can be presented during the chartering phase.

Example: Work products from the EPDP Team on the Temporary Specification for gTLD Registration Data

Project Status & Condition Assessment:

The WG leadership, in collaboration with the WG support staff and the GNSO Council liaison, shall assess the Status and Condition of the project at least once a month. Such frequency is required in preparation for the GNSO Council monthly meeting, where At-Risk or In-Trouble projects are subject to review by GNSO Council leadership, and in some instances may be deliberated by the full GNSO Council.

The WG leadership, in collaboration with the WG support staff and the GNSO Council Liaison, shall use an escalation procedure (see Guidance documents below), which defines specific conditions that trigger the execution of a repeatable mitigation plan. The objective of this exercise is to return the project to an acceptable state ultimately achieving its planned outcomes.

Guidance: Project Status and Condition Change Procedure

Project Change Request:

The WG shall submit a Project Change Request (PCR) Form to the GNSO Council when its deliverable and baseline delivery date are revised. The PCR shall include a rationale for why these changes were made, their impacts on the overall timeframe of the PDP or any other interdependencies, and a proposed remediation plan.

The use of the PCR mostly occurs when primary deliverable dates are changed due to unforeseen or extreme circumstances. However, it can also be used to document changes in the deliverable requirements that may not have been identified in the chartering process.

When the PCR is required, it should be completed by the WG leadership team and it will likely be presented to the GNSO Council for approval.

Guidance: Project Change Request Form
Example: Project Change Request Form submitted by the EPDP Team on the Temporary Specification for gTLD Registration Data

Resources Tracking:

The purpose for resource tracking is to deliver its work according to the work plan and be responsible for managing these resources.

For projects where dedicated funds are provided outside of budgeted policy activities, the WG shall provide regular budget versus actual expense reporting updates using a GNSO approved tool to allow for a better tracking of the use of resources and budget.

Guidance: GNSO Project Work Product Catalog

Instruction for Charter Drafting Team
Upon project scope definition, the Charter Drafting Team shall estimate the community resources and financial budget, if applicable (for example, external legal advice or mediation services, face-to-face meetings, etc.), that the WG needs.

Note, however a completed project plan will not usually occur until after a working group has performed a cursory review of the in-scope issues and confirmed its work plan. Therefore, the formal project plan should be returned back to the GNSO Council for final confirmation and formal initiation of the project Status, Condition, and Delivery Date.

Please include any work products for resource tracking purposes that can be produced during the chartering phase.

Section IV: Formation, Staffing, and Organization

Working Group Model:

Instruction for Charter Drafting Team
Please specify which model the WG will use, with options including but not limited to:

- Open Model
- Representative Model (Full Community)
- Representative & Open Model

Please provide detailed rationale for the chosen Working Group model.

Guidance: A Comparison Table of Working Group Models

[The WG will use a Representative Model. Please see the Membership Structure Section, below, for further details.]

Membership Structure:

Instruction for Charter Drafting Team
Please provide a detailed description of the composition of the working group membership, including members, participants, and/or observers, as applicable.

Please specify how an observer becomes a member, if applicable.

Guidance: A Comparison Table of Working Group Models
Example: Charter of the EPDP Team on the Temporary Specification for gTLD Registration Data

[Notes from Transfer Policy Review Scoping Team:

"The Scoping Team anticipates that not all SGs/Cs within the GNSO will have interest in this policy issue, but the Scoping Team is concerned about lack of participation in the eventual PDP. To that end, the Scoping Team asks the GNSO Council to consider including "represented Observers" for those groups that do not wish to participate fully or nominate active WG members. The assigned Observers would be required to monitor the WG's discussions, potential recommendations, and timeline of milestones. The represented Observers would also be required to keep their respective groups informed of the WG's status and upcoming milestones. While some GNSO SGs/Cs may not have active WG members, the goal of requiring represented Observers is to ensure all groups will be fully informed when the GNSO Council starts to consider the policy recommendations."]

ICANN org would recommend the GNSO Council consider a member/alternate/observer model*, comprised of:

Members, who are responsible for active participation, preliminary deliberations, and consensus;
Alternates, who only participate if a Member is not available, but will be responsible for keeping up with all relevant WG deliberations to ensure they remain informed and can contribute when needed;
Observers - who may actively follow the work of the Transfer Policy WG, but will not have posting or speaking rights during WG meetings.

Note: ICANN org is recommending limiting the membership of the WG to assist in preventing an oversized, and potentially inefficient, WG.

The Membership Structure of the Transfer Policy Review Working Group will be composed of Members, Alternates, Observers, and a dedicated GNSO Council Liaison. Observers will be allowed to follow the work of the Working Group, but will not be authorized to speak up during meetings or post to the Working Group list; these observers are asked to coordinate through their group's appointed Members, and, of course, may respond to all public comment proceedings.

With respect to the number of Members and Alternates, Staff would recommend that following publication of the Final Issue Report, and assuming the GNSO Council initiates a PDP, the GNSO Council would contact SO/AC/SG/Cs to inquire about expected participation, including how many members should be appointed per group.

Description of Transfer Policy Review Working Group roles:

- **WG Members**: Members are expected to commit to the Statement of Participation as well as participate in any WG consensus calls, as applicable. Members are required to represent the formal position of their appointing organization, not individual views or positions.

  *NOTE: the Scoping Team discussed the participation of a "represented Observer," or a participant who would be responsible for following the WG's discussions, potential recommendations, and timeline of milestones. The idea of the represented Observer was to allow for GNSO SG/Cs (and outside SOs/ACs, if applicable) who are not interested and/or do not have prospective members able to fully commit to the responsibilities and requirements of active Members. These groups would be required to put forward at least one individual who would be responsible for following the work of the WG and keeping their respective group informed. Because this concept is not explicitly recognized in the PDP 3.0 manual, ICANN org is recommending that each GNSO SG/C nominate at least one member to participate. In the event a GNSO SG/C is unable to nominate a member, ICANN org would recommend at least one observer (defined below) be responsible for keeping their respective SG/C informed of

milestones and potential recommendations that may affect the SG/C. The WG could consider quarterly webinars/info sessions to assist in the observers' understanding of the status, timeline, upcoming milestones, and draft recommendations.

- **WG Observers**: Anyone interested in this effort may join as an observer – observers are subscribed to the mailing list on a read-only basis but are NOT able to post. Similarly, observers are NOT invited to participate in WG meetings. The ability to listen in real-time as well as recordings / transcripts of meetings will be available to observers.
- **Alternates**: Alternates will only participate if a Member is not available. Alternates will be responsible for keeping up with all relevant WG deliberations to ensure they remain informed and can contribute when needed.
- **GNSO Council Liaison**: The GNSO Council shall appoint a liaison who is accountable to the GNSO. The liaison must be a member of the Council, and the Council recommends the liaison be a Council member able to serve during the life of this WG. Generally speaking, the liaison is expected to fulfill the liaison role in a neutral manner, monitor the discussions of the Working Group and assist/ inform the Chair and the WG as required.

Additional Notes - Consider for Inclusion by Charter Drafting Team
The GNSO Secretariat should circulate a 'Call For Volunteers' in accordance with the group structure determined by the GNSO Council or this Charter drafting team:

- Publication of announcement on relevant ICANN web sites including but not limited to the GNSO and other Supporting Organizations and Advisory Committee web pages; and
- Distribution of the announcement to GNSO Stakeholder Groups, Constituencies and other ICANN Supporting Organizations and Advisory Committees

The standard WG roles, functions & duties shall be applicable as specified in Section 2.2 of the Working Group Guidelines.

Membership Criteria:

A. Expected Skills for Working Group Members
WG members shall review the full text of the Guidance document below to understand the responsibilities and skills that they are expected to have in order to fully participate in the WG activities.

Guidance: Working Group Member Skills Guide

Working Group Members and Alternates must possess:

- Knowledge of Transfer Policy issue background and current work status (technical knowledge of inter-registrar transfers is strongly preferred;
- Commitment to participating in Working Group meetings on a regular and ongoing basis;
- Ability to create factual, relevant and easily understandable messages, and able to succinctly deliver them to the Working Group;
- Ability to deliver a point constructively and concisely;
- Familiarity with the following sections of the Working Group Guidelines:
  - Section 4.1 Session Planning – General Meeting Logistics
  - Section 4.2 Communication/Collaboration Tools
- Effective oral, written, and interpersonal communication skills (in simple, comprehensible English);
- Research skills with the ability to discern factual, factually relevant, and persuasive details and sources;

- Commitment to manage a diverse workload, while collaborating with a Working Group of individuals with different backgrounds and interests in driving objectives;
- In depth knowledge of Working Group discussions, actions taken at meetings, and deliverables;
- Understanding of the perspectives and interests of the members' own stakeholder group or constituency;
- Project management skills in driving the completion of SG/C statements in a timely manner.

Instruction for Charter Drafting Team

Please provide a description of expected responsibilities for WG members that need to be highlighted in the charter, including associated skills required and available resources to carry out these responsibilities.

If specific expertise is needed or required for members, please specify whether any independent evaluation needs to be carried out to confirm that members have required expertise.

B. Joining of New Members After Project Launch

The existing practice as stated in the Working Group Guidelines is that anyone can join a WG at any point as long as they get up to speed and do not reopen previously closed topics, unless they provide new information. Nonetheless, the Working Group Guidelines do not prevent WG leadership from deciding, in consultation with the WG, whether new members can be accepted after the start of the WG effort.

As a representative model is recommended, new members would only join after the launch of the PDP if a current member is no longer able to continue in its membership, and no alternates are available to fill in. New WG members should be mindful that, once input/comment periods have been closed, discussions or decisions should not be resurrected unless there is group consensus that the issue should be revisited in light of new information that has been introduced. If the reopening is perceived as abusive or dilatory, a WG member may appeal to the Chair.

Guidance: Criteria for Joining of New Members After a PDP Working Group is Formed or Rechartered

Instruction for Charter Drafting Team

If applicable, please specify:

- The circumstances that new membership may be suspended;
- The exceptional cases that new members can join after the WG is formed.

C. Experts Contributors

Expert contributors are not expected to participate in any consensus designation process, but provide perspective/expertise/knowledge to the PDP WG.

The Council may be able to use an independent evaluation process (e.g., GNSO Council Standing Selection Committee) to confirm whether those individuals have demonstrated the expertise/knowledge/perspective.

Instruction for Charter Drafting Team
Please specify if the GNSO Council wishes to run an open call for expert contributors in order to recruit individuals who have expertise, knowledge, and/or perspective that otherwise would not be present in the PDP.

Leadership Structure:

Instruction for Charter Drafting Team
Please provide a description of the leadership structure of the WG, including the mechanism for selecting/confirming the Chair/Vice-Chair(s)/Co-Chairs(s), as applicable.

Guidance: A Comparison Table of Working Group Models
Example: Charter of the EPDP Team on the Temporary Specification for gTLD Registration Data

Leadership Criteria:

WG leaders shall review the full text of the Guidance document below to understand the expectations for WG leaders, including their role & responsibilities as well as minimum skills/expertise required.

In short, a WG leader is expected to:

- Encourage representational balance
- Encourage adherence to ICANN's Expected Standards of Behavior & Community Anti-Harassment Policy
- Ensure WG documents represent the diversity of views
- Make consensus designation on working group recommendations
- Handle working group complaint process
- Be versed in GNSO Operating Procedures
- Assume a neutral and impartial role
- Build consensus
- Balance working group openness with effectiveness
- Make time commitment

[The GNSO Council will appoint a qualified Chair for the WG. Below is a description of the qualifications and role of the Chair for this WG. The WG, once formed, will select one or two Vice Chairs to assist the Chair. Should at any point a Vice Chair need to step into the role of Chair, the same expectations with regards to fulfilling the role of chair as outlined in this charter will apply. The GNSO Council leadership and Standing Selection Committee leadership will jointly review the responses and will propose a Chair to the GNSO Council which will then either affirm the selection or reject the selection and send the process back to the GNSO Council leadership and Standing Selection Committee leadership.

The Expression of Interest should address the following issues:

- What is the applicant's interest in this position?
- What particular skills and attributes does the applicant have that will assist him/her in chairing the WG?
- What is the applicant's knowledge of the Transfer Policy?
- What is the applicant's experience in and knowledge of the GNSO Policy Development Process and domain name registration process as it relates to ICANN?
- Is the applicant able to commit the time required and necessary work needed to chair the PDP?

- Conflict of Interest Statement – does the applicant have any affiliation with or involvement in any organization or entity with any financial or non-financial interest in the subject matter of this PDP?
- Also expected to be included:
    - A link to an up-to-date Statement of Interest (SOI) - https://community.icann.org/x/c4Lg o A statement confirming your commitment and ability to act neutrally.

As outlined in the GNSO Working Group Guidelines (WGG), the purpose of a Chair is to call meetings, preside over working group deliberations, manage the process so that all participants have the opportunity to contribute, and report the results of the Working Group to the Chartering Organization. These tasks require a dedicated time commitment as each week calls have to be prepared, the agenda concretized, and relevant material reviewed. The Chair shall be neutral. While the Chair may be a member of any group which also has representation on the Working Group, the Chair shall not act in a manner which favors such group. The Chair shall not be a member of the Working Group for purposes of consensus calls.

In addition, it is expected – that interested candidates shall have considerable experience in chairing working groups, and direct experience with at least one GNSO Policy Development Process throughout its lifecycle. Familiarity with the functioning of a Working Group is important to understand the various leadership skills that are necessary to employ during a WG's lifecycle. For example, a Chair has to ensure that debates are conducted in an open and transparent matter and that all interests are equally and adequately represented within the Group's discussions. During the later stages of a WG when recommendations are drafted, a Chair will benefit from understanding the viewpoints of various participants to ensure that an acceptable and effective outcome – ideally in the form of consensus – can be achieved.

In short, a WG Chair is expected to:
i. Attend all PDP Team meetings to assure continuity and familiarity with the subject matter and the ongoing discussions;
ii. Prepare meetings by reading all circulated materials;
iii. Be familiar with the subject matter, including but not limited to GDPR and other relevant topics, and actively encourage participation during the calls;
iv. Be active on the PDP mailing list and invite PDP WG members and liaisons to share their viewpoints;
v. Drive forward the PDP WG and assure that discussions remain on point;
vi. Work actively towards achieving policy recommendations that ideally receive full consensus;
vii. Ensure that particular outreach efforts are made when community reviews are done of the group's output;
viii. Underscore the importance of achieving overall representational balance on any sub-teams that are formed;
ix. Encourage and, where necessary, enforce the ICANN Standards of Behavior and Community Anti-Harassment Policy;
x. Coordinate with and ensure that the WG is supported as effectively as possible; and
xi. Conduct consistent, adequate and timely reporting to the GNSO Council on the progress of the PDP.

Finally, as also pointed out in the GNSO Working Group Guidelines, 'appointing a co-chair(s) or vice-chair(s) may facilitate the work of the Chair by ensuring continuity in case of absence, sharing of workload, and allowing the Chair to become engaged in a particular debate.' As a result, similar tasks and skills are expected from vice-chair(s), although the overall workload may be reduced as a result of being able to share this with the Chair.]

Guidance: Expectations for Working Group Leaders that Outline Role & Responsibilities as well as Minimum Skills / Expertise Required

Instruction for Charter Drafting Team
Please provide a description of role & responsibilities and skills/expertise required for WG leaders that need to be highlighted in the charter.

If Expressions of Interest will be sought for WG leaders, please include the relevant text in the request for Expressions of Interest in this section.

Example: Charter of the EPDP Team on the Temporary Specification for gTLD Registration Data

Leadership Review:

WG leadership shall review the full text of Guidance documents below to understand the regular review of WG leadership performance by the GNSO Council, as well as the member survey that feeds into the review.

Guidance: Regular Review of PDP Working Group Leadership by GNSO Council & PDP Working Group Member Survey on Leadership Performance

Instruction for Charter Drafting Team
Please provide the expected frequency and timeframe for the WG leadership review, including the expected timeframe for the PDP WG member survey on leadership performance.

Additional Notes - Consider for Inclusion by Charter Drafting Team

The review of PDP WG leadership provides a regular opportunity for the GNSO Council to check in with PDP WG leadership and liaisons to identify resources or input that Council may need to provide, as well as opportunities for the leadership team to improve. The review also enables the GNSO Council to work with the PDP WG leadership and Council liaison to develop and execute a plan to address possible issues/opportunities identified.

The schedule of reviews will be established in the charter of each PDP WG and will likely be different for each depending on the length, complexity, and structure of the PDP. Reviews may also be initiated by Council leadership and/or the Council liaison to the WG in response to circumstances indicating that a review is necessary.

The following is a non-exhaustive list of issues that Council leadership and Council liaison could seek to address in the review process.

- There is substantial evidence that the PDP WG leadership team or an individual on the PDP WG leadership team:
  - Has difficulty facilitating goal-oriented WG meetings aligned with the requirements of the WG's charter and workplan.
  - Is unable to effectively manage WG members' disruptive behaviors, and this is negatively impacting the ability of the WG to complete its work or is discouraging participation by a diverse set of members.

- Is consistently unable to keep the WG on track to meet target deadlines.
- Does not communicate effectively with WG members or respond to concerns raised by members.
- Does not act in a neutral, fair, and objective manner in the context of the WG, for example by advocating for his or her own agenda or discouraging perspectives with which he or she disagrees.

- The Council leadership and Council liaison may further want to consider whether members of the PDP WG leadership team are able to work together effectively in a collegial manner as they manage the WG and communicate with members.

Feeding into the regular review of PDP WG leadership by the GNSO Council, an anonymous survey will be conducted in advance of the scheduled review so that the results can be taken into account. The survey will be distributed electronically at regular intervals by the GNSO Council to PDP WG members. The survey will be open for at least one week. The exact interval at which the survey is conducted will be different per WG and may be tied to the length of the WG's timeline or specific milestones included in the charter. Specific triggers may also be identified that will result in the launch of a survey.

GNSO Council Liaison

The GNSO Council shall appoint a liaison who is accountable to the GNSO. The liaison must be a member of the Council, and the Council recommends that the liaison should be a Council member and be able to serve during the life of this WG.

The liaison shall review the Guidance documents below.

Guidance: New Liaison Briefing and Liaison Handover & GNSO Council Liaison Supplemental Guidance

Role of the GNSO Council Liaison

[In addition:

- The liaison shall serve as an interim WG Chair until a Team Chair is named. As per current practice, it would not be appropriate for the liaison to be considered for a permanent Chair or co-chair/vice-chair position;
- The liaison is expected to report to the GNSO Council on a regular basis (at a minimum, at or before the monthly meetings of the GNSO Council and as issues or significant milestones arise in the group's work) on the progress of the Working Group. Such report is expected to be coordinated with the PDP WG leadership;
- The liaison will assist the PDP WG Chair as required with his/her knowledge of policy development processes and practices;
- The liaison will refer to the GNSO Council any questions or queries the PDP WG might have in relation to its charter and mission;
- The liaison will assist or engage when the PDP WG faces challenges or problems, and will notify the GNSO Council of efforts in this regard;
- The liaison will assist the WG Chair in suspected cases of abuse of ICANN's Expected Standards of Behavior, ICANN's Community Anti-Harassment Policy and/or restricting the participation of someone who seriously disrupts the WG;
- The liaison will facilitate in case there is disagreement between the PDP WG Chair and PDP WG member(s) in relation to designation of consensus given to certain recommendations;

- The liaison is expected to be a regular attendee/participant of PDP WG meetings;
- The liaison is expected to fulfill his/her role in a neutral manner. It would not be appropriate for the liaison to intervene or participate in PDP WG deliberations in his or her personal capacity; the liaison is expected to channel such comments through the representatives of his or her Stakeholder Group, and to only speak on calls and meetings in their official liaison capacity;
- The GNSO Council liaison is responsible for ensuring that the PDP WG Chair is informed about activities of the GNSO Council that have an impact on the PDP WG. This includes not only actions taken with respect to substance related to the WG, but also any actions taken on matters upon which the Team depends or on which the Council depends on the WG;
- The GNSO Council liaison should participate in regular meetings with the PDP WG Leadership and consult with PDP WG Leadership prior to providing updates or reports to the GNSO Council; and,
- The GNSO Council liaison should be the person upon whom the Team relies to convey any communications, questions or concerns to the GNSO Council. Taking into account the role and responsibilities of the liaison identified above, the GNSO Council furthermore expects that the liaison:
    - Will stay up-to-date on the deliberations in order to be in a position to provide the GNSO Council with adequate updates at appropriate times;
    - Only participate in the PDP in their official liaison capacity;
    - Is alert to situations that may require liaison involvement and be prepared to act swiftly, as and when needed;
    - Will notify the GNSO Council as soon as is practical if he/she is no longer able to take on these responsibilities so that another liaison can be identified; and
    - Will notify the Council in a timely manner should there be any adjustment to the work plan and, in particular, any delay that may be likely to occur in adhering to the agreed PDP milestones.]

Instruction for Charter Drafting Team
Please provide a description of role & responsibilities for GNSO Council liaison to the WG that need to be highlighted in the charter here.

Example: Charter of the EPDP Team on the Temporary Specification for gTLD Registration Data

Additional Notes - Consider for Inclusion by Charter Drafting Team
The liaison shall complete the following actions for onboarding purposes:

- Review the GNSO Council liaison to the WGs - Role Description;
- Review the New Liaison Briefing and Liaison Handover document;
- Consult the supplemental guidance developed to provide more precision in their responsibilities and the frequency in which they must be carried out;
- Familiarize with the provisions of the GNSO Operating Procedures relevant to liaisons;
- Subscribe to the PDP mailing lists and relevant sub teams;
- Subscribe to the PDP Leadership mailing list(s), if applicable. In addition, add o the PDP Leadership Skype chat (or other communication channel) if applicable;
- Consider requesting a catch up call with the relevant GNSO policy support staff. This call should clarify the role of the liaison in terms of PDP conference call attendance, expected responsibilities and an update as to the current status of the PDP if already in operation (milestones and anticipated hurdles);
- Review links to the wiki workspaces and mailing list archives via email;

- (If the PDP is already in operation) Consider requesting that PDP Leadership and the outgoing liaison(s) share relevant briefing documents specific to the PDP, to highlight the scope of the PDP charter, current status, timeline, milestones, problem areas/challenges, anticipated hurdles, etc;
- (If the PDP is already operation) Participate in an onboarding conference call with the incoming and outgoing liaisons as well as PDP Leadership; GNSO policy support staff will also be present on the call.

Importantly, the liaison is expected to fulfil his/her role in a neutral manner. This means that everything the liaison does during his/her tenure, including but not limited to participating in WG calls, reporting status, conveying information, and escalating issues, should be done in that neutral manner.

In short, the GNSO Council liaison is expected to:

- Fulfill liaison role in a neutral manner
- Be a regular participant of WG meetings
- Participate in regular meetings with WG leadership
- Report to Council on the WG progress
- Serve as an interim WG Chair until a Chair is named
- Convey to Council on WG communications, questions, concerns
- Inform WG leadership about Council activities impacting the WG
- Refer to Council questions related to WG Charter
- Assist or engage when WG faces challenges
- Assist in case of abuse of ICANN's Expected Standards of Behavior
- Assist with knowledge of WG processes and practices
- Facilitate when there is disagreement regarding consensus designation
- Facilitate when a Section 3.7 Complaint Process is invoked

Support Staff:

The ICANN org staff assigned to the WG will fully support the work of the Working Group as requested by the Chair including meeting support, document drafting, editing and distribution and other substantive contributions when deemed appropriate.

Staff assignments to the Working Group:

- GNSO Secretariat
- ICANN policy staff members

Section V: Rules of Engagement

Statements of Interest (SOI) Guidelines:

Each member of the WG is required to submit an SOI in accordance with Section 5 of the GNSO Operating Procedures.

Statement of Participation:

Each member of the WG must acknowledge and accept the Statement of Participation (as provided below), including ICANN's Expected Standards of Behavior, before he/she can participate in the WG.

Statement of Participation

As a member of the [name of group]:

- I agree to genuinely cooperate with fellow members of the [group] to reach consensus on the issues outlined in the Charter. I understand this does not mean that I am unable to fully represent the views of myself or the organization I represent but rather, where there are areas of disagreement, I will commit to work with others to reach a compromise position to the extent that I am able to do so;
- I acknowledge the remit of the GNSO to develop consensus policies for generic top level domains. As such, I will abide by the recommended working methods and rules of engagement as outlined in the Charter, particularly as it relates to designating consensus and other relevant rules in GNSO Working Group Guidelines;
- I will treat all members of the [group] with civility both face-to-face and online, and I will be respectful of their time and commitment to this effort. I will act in a reasonable, objective, and informed manner during my participation in this [group] and will not disrupt the work of the [group] in bad faith;
- I will make best efforts to regularly attend all scheduled meetings and send apologies in advance when I am unable to attend. I will take assignments allocated to me during the course of the [group] seriously and complete these within the requested timeframe. [If applicable] As and when appropriate I shall seek to be replaced by my designated Alternate in accordance with the wishes of my appointing organization;
- I agree to act in accordance with ICANN Expected Standards of Behavior, particularly as they relate to:
    - Acting in accordance with, and in the spirit of, ICANN's mission and core values as provided in ICANN's Bylaws;
    - Listening to the views of all stakeholders and working to build consensus; and
    - Promoting ethical and responsible behavior;
- I agree to adhere to any applicable conflict of interest policies and the Statement of Interest (SOI) Policy within the GNSO Operating Procedures, especially as it relates to the completeness, accuracy, and timeliness of the initial completion and maintenance of my SOI; and
- I agree to adhere to the ICANN Community Anti-Harassment Policy and Terms of Participation and Complaint Procedures.

I acknowledge and accept that this Statement of Participation, including ICANN's Expected Standards of Behavior, is enforceable and any individual serving in a Chair role (such as Chair, Co-Chair, or Acting Chair or Acting Co-Chair) of the [group] and GNSO Council Leadership Team have the authority to restrict my participation in the [group] in the event of non-compliance with any of the above.

Problem/Issue Escalation & Resolution Process:

Please reference Sections 3.4 and 3.5 of the Working Group Guidelines and the Guidance document below.

Guidance: Guidelines Concerning ICANN Org Resources for Conflict Resolution and Mediation

Instruction for Charter Drafting Team
As the GNSO Council may modify the problem/issue escalation & resolution process at its discretion, please include additional resources and mechanisms, if any.

Formal Complaint Process:

Please reference Section 3.7 of the Working Group Guidelines and the Guidance document below. The Complaint Process may be modified by the GNSO Council at its discretion.

Guidance: Clarification to Complaint Process in GNSO Working Group Guidelines

Section VI: Decision Making Methodologies

Consensus Designation Process:

Section 3.6 of the GNSO Working Group Guidelines, as included below, provides the standard consensus-based methodology for decision making in GNSO WGs.

Section 3.6 notably refers to the 'Chair' (singular) of a WG, which does not conform to the reality of current PDP WG leadership structures. References to 'Chair' shall include PDP WG Co-Chairs and/or Vice Chair(s) that form the WG leadership, if applicable.

WG leaders, members and liaison shall review the Consensus Playbook (Guidance document below) which provides a structured approach for consensus building and providing behavior insights, tools, and techniques to bridge differences, break deadlocks, and find common ground.

Guidance: Consensus Playbook

3.6 Standard Methodology for Making Decisions

The Chair will be responsible for designating each position as having one of the following designations:

- **Full consensus** - when no one in the group speaks against the recommendation in its last readings. This is also sometimes referred to as **Unanimous Consensus.**
- **Consensus** - a position where only a small minority disagrees, but most agree. *[Note: For those that are unfamiliar with ICANN usage, you may associate the definition of 'Consensus' with other definitions and terms of art such as rough consensus or near consensus. It should be noted, however, that in the case of a GNSO PDP originated Working Group, all reports, especially Final Reports, must restrict themselves to the term 'Consensus' as this may have legal implications.]*
- **Strong support but significant opposition** - a position where, while most of the group supports a recommendation, there are a significant number of those who do not support it.
- **Divergence** (also referred to as **No Consensus**) - a position where there isn't strong support for any particular position, but many different points of view. Sometimes this is due to irreconcilable differences of opinion and sometimes it is due to the fact that no one has a

particularly strong or convincing viewpoint, but the members of the group agree that it is worth listing the issue in the report nonetheless.

- **Minority View** - refers to a proposal where a small number of people support the recommendation. This can happen in response to a **Consensus**, **Strong support but significant opposition**, and **No Consensus;** or, it can happen in cases where there is neither support nor opposition to a suggestion made by a small number of individuals.

In cases of **Consensus**, **Strong support but significant opposition**, and **No Consensus**, an effort should be made to document that variance in viewpoint and to present any **Minority View** recommendations that may have been made. Documentation of **Minority View** recommendations normally depends on text offered by the proponent(s). In all cases of **Divergence,** the WG Chair should encourage the submission of minority viewpoint(s).

The recommended method for discovering the consensus level designation on recommendations should work as follows:

i. After the group has discussed an issue long enough for all issues to have been raised, understood and discussed, the Chair, or Co-Chairs, make an evaluation of the designation and publish it for the group to review.
ii. After the group has discussed the Chair's estimation of designation, the Chair, or Co-Chairs, should reevaluate and publish an updated evaluation.
iii. Steps (i) and (ii) should continue until the Chair/Co-Chairs make an evaluation that is accepted by the group.
iv. In rare case, a Chair may decide that the use of polls is reasonable. Some of the reasons for this might be:
    - A decision needs to be made within a time frame that does not allow for the natural process of iteration and settling on a designation to occur.
    - It becomes obvious after several iterations that it is impossible to arrive at a designation. This will happen most often when trying to discriminate between **Consensus** and **Strong support but Significant Opposition** or between **Strong support but Significant Opposition** and **Divergence.**

Care should be taken in using polls that they do not become votes. A liability with the use of polls is that, in situations where there is **Divergence** or **Strong Opposition**, there are often disagreements about the meanings of the poll questions or of the poll results.

Based upon the WG's needs, the Chair may direct that WG participants do not have to have their name explicitly associated with any Full Consensus or Consensus view/position. However, in all other cases and in those cases where a group member represents the minority viewpoint, their name must be explicitly linked, especially in those cases where polls where taken.

Consensus calls should always involve the entire Working Group and, for this reason, should take place on the designated mailing list to ensure that all Working Group members have the opportunity to fully participate in the consensus process. It is the role of the Chair to designate which level of consensus is reached and announce this designation to the Working Group. Member(s) of the Working Group should be able to challenge the designation of the Chair as part of the Working Group discussion. However, if disagreement persists, members of the WG may use the process set forth below to challenge the designation.

If several participants[38] in a WG disagree with the designation given to a position by the Chair or any other consensus call, they may follow these steps sequentially:

1. Send email to the Chair, copying the WG explaining why the decision is believed to be in error.
2. If the Chair still disagrees with the complainants, the Chair will forward the appeal to the CO liaison(s). The Chair must explain his or her reasoning in the response to the complainants and in the submission to the liaison. If the liaison(s) supports the Chair's position, the liaison(s) will provide their response to the complainants. The liaison(s) must explain their reasoning in the response. If the CO liaison disagrees with the Chair, the liaison will forward the appeal to the CO. Should the complainants disagree with the liaison support of the Chair's determination, the complainants may appeal to the Chair of the CO or their designated representative. If the CO agrees with the complainants' position, the CO should recommend remedial action to the Chair.
3. In the event of any appeal, the CO will attach a statement of the appeal to the WG and/or Board report. This statement should include all of the documentation from all steps in the appeals process and should include a statement from the CO[39].

Instruction for Charter Drafting Team
If the GNSO Council wishes to deviate from the standard methodology for making decisions or empower the WG to decide its own decision-making methodology, this section should be amended as appropriate.

Who Can Participate in Consensus Designation:

Instruction for Charter Drafting Team
Please specify who from the WG membership can participate in the consensus designation process, including appropriate weight to the position held by such member(s), if applicable, and any factors that the WG leadership shall consider in assessing consensus.

Guidance: A Comparison Table of Working Group Models
Example: Charter of the EPDP Team on the Temporary Specification for gTLD Registration Data

Termination or Closure of Working Group:

Typically, the WG will close upon the delivery of the Final Report, unless assigned additional tasks or follow-up by the GNSO Council.

[38] Any Working Group member may raise an issue for reconsideration; however, a formal appeal will require that that a single member demonstrates a sufficient amount of support before a formal appeal process can be invoked. In those cases where a single Working Group member is seeking reconsideration, the member will advise the Chair and/or liaison of their issue and the Chair and/or liaison will work with the dissenting member to investigate the issue and to determine if there is sufficient support for the reconsideration to initial a formal appeal process.

[39] It should be noted that ICANN also has other conflict resolution mechanisms available that could be considered in case any of the parties are dissatisfied with the outcome of this process.

The GNSO Council may terminate or suspend the WG prior to the publication of a Final Report for significant cause such as changing or lack of community volunteers, the planned outcome for the project can no longer be realized, or when it is clear that no consensus can be achieved.

Guidance: Project Status and Condition Change Procedure

Section VII: Change History

Instruction for Charter Drafting Team
Please document any significant changes to the WG charter in this section, including, but not limited to:

- Mission, purpose & deliverable
- Formation, staff & organizational

Section VIII: Charter Document History

Version	Date	Description
1.0		

Staff Contact:	<Enter staff member name>	Email:	Policy-Staff@icann.org

Translations: If translations will be provided please indicate the languages below:											

Annex B Contracted Party TechOps Transfers White Paper

New gTLD Transfer Process

v.02 CPH TechOps Discussion Paper

Abstract

Changes in the WHOIS system resulted from the GDPR legislation that went into effect on 26 May 2018. These changes impacted the ability for ICANN Accredited Registrars to facilitate the process of inter-registrar domain name transfers, as the WHOIS, prior to GDPR, played a critical role in validation and communication steps that had been in place to meet certain compliance requirements while ensuring reliable and reasonable confirmation of the transfer and parties involved. With WHOIS changing, the gTLD registrar transfer process and compliance requirements from ICANN that registrars must meet required modification in order to preserve the overall inter-registrar transfer functionality..

After an in-depth discussion, the Contracted Party House (CPH) TechOps group ("CPH TechOps") reviewed the impacts, and suggested an interim solution[40] on 1 May 2018 which was included into the Temporary Specification for gTLD registration data[41] as Annex G, issued 17 May 2018.

Since the Temporary Specification supersedes all other relevant ICANN policies in regard to transfers, Annex G now governs the gTLD transfer process for the duration of the Temporary Specification, which can be upheld for a maximum of 12 months.

[40] https://www.icann.org/en/system/files/correspondence/sattler-to-atallah-01may18-en.pdf
[41] https://www.icann.org/resources/pages/gtld-registration-data-specs-en

At the GDD Summit[42] in Vancouver in May 2018, the CPH TechOps group convened two workshops to explore what a new transfer policy could look like in light of the GDPR.

Though no final transfer process was developed, the attendees agreed on a set of high-level principles that should guide the further discussion.

These principles are:

- The transfer process must comply with current data privacy regulations
- The transfer process must be instant, however a time to validate the legitimacy of transfer should be given
- A transfer token shall be sufficient to authorize a transfer
- No personal data shall be transferred from the old to the new Registrar
- The existing gTLD transfer policy should be changed as little as possible

At ICANN 63[43] in Barcelona,October 2018 the CPH TechOps group held a workshop based on the discussion of the "New gTLD Transfer Process CPH Discussion Paper v.01"[44]. Four topics were worked upon in detail:

1. **Who is responsible for Transfer Token & TTL handling/storage/processing — Registrar/Registry/both?**

   Since the Transfer Token/AuthCode and the corresponding TTL are the central elements in the proposed new transfer process it was concluded that, to reach a uniform, transparent, and predictable process, Registries should be in control of the storage and processing of the AuthCode, regarding the technical part. To be able to roll this security policy implementation out to all Registries and Registrars there could be a very narrow (fast track) policy process rendering the technical flow into binding policy.

[42] https://www.icann.org/gddsummit
[43] https://meetings.icann.org/en/barcelona63
[44] New gTLD Transfer Process CPH Discussion Paper v.01

It was also concluded that, while the policy process and implementation of such is underway, the Transfer Token/AuthCode should be set by the Registrar according to a to-be-developed best practice.

This provisional behaviour will be outlined below in addition to the new process, and shall cease to exist once the new policy is implemented.

2. **Should the transfer check of the Losing Registrar be mandatory or optional?**

The group agreed that the requirement to notify the Registrant about a transfer request should be mandatory. As general business practises of Registrars and individual transfer scenarios vary, the group concluded that such notification does not have to be an email, but rather may incorporate other means of more modern communication.

To increase security the group suggest that only the registrant should be able to request a transfer; this would eliminate the admin contact acting as another party who is able to approve or request transfers.

3. **Do we need a process in case the Losing Registrar is not responding? Should there be a ccTLD-like Registry involvement?**

Due to the importance of the cooperation of the Losing Registrar in a Transfer scenario the group was unanimously in favor of having such a process.

After deliberating in depth about the possibilities of a ccTLD-like Registry involvement, it was found that because of potential GDPR restrictions as well as legal and language reasons a gTLD Registry would very likely not be able to perform such service in a manner satisfying for all parties.

As the expected behavior of the Losing Registrar is mandated by ICANN policy the lack of responsiveness constitutes a deviation from such and should hence be dealt with via an ICANN Compliance Process.

To discourage premature/frivolous compliance requests which may pose an extraordinary burden on the ICANN Compliance team it was concluded that only the Gaining Registrar should be able to invoke such a process. It was also agreed that before opening a case the Gaining Registrar must try to resolve the issue with the Losing Registrar via the TEAC directly

4. **Possible values for the TTL i.e 1 to 15 days or 1 hour to 30 days …. Do we need a policy/best practice about the syntax of a transfer token (length, characters)? Should we use the term transfer token or AuthCode, do we need a definition?**

   The group was in agreement that the term describing the transfer password should be AuthCode, as this term is already in use and well known. It was also agreed that there must be a policy to manage the syntax of the AuthCode as well as the allowed values of the TTL.

   In regard to the TTL the group suggested a validity of no more than 14 days, presented as the total number of hours until TTL expiration. There was no resolution for a minimum TTL requirement, because registrars with different business models may have different requirements for how quickly a domain name gets unlocked and transferred.

   More work on any of these topics is needed.

To advance the discussion, the following text describes a new transfer process in adherence to the high-level principles and findings of the workshop.

Overview

The gTLD Registrar transfer process can be divided into three distinct phases:

1. Registrant initiates domain name transfer process with Losing Registrar
2. Registrant requests domain name transfer with Gaining Registrar
3. Registry transfers domain name from Losing Registrar to Gaining Registrar

For each of the phases, every involved party has to adhere to a defined set of policies and technical transactions.

Transfer Phases

3.1. Registrant initiates domain name transfer

Flow

- Registrant requests issuance of an AuthCode from Losing Registrar
- Losing Registrar verifies AuthCode request
- Losing Registrar checks Client Transfer Lock
- Losing Registar checks Server Transfer Lock
- Losing Registrar verifies no applicable Registrant changes within last 60 days
- If no Transfer Lock is set AuthCode request proceeds
- Losing Registrar sets AuthCode & TTL via EPP in Registry system
- Losing Registrar communicates AuthCode & TTL to the registrant

Policy

The Losing Registrar MUST verify the authenticity of the AuthCode request according to their internal policies and practices (which may vary depending on the business model). This MUST involve a notification to the current registrant contact[45] through a medium (email, phone, messenger, etc.) of the Registrar's choosing sent at the time when the request is made. Once those required steps are completed, the AuthCode must be issued to the requestor within five

[45] https://www.icann.org/resources/pages/foa-registrar-transfer-confirmation-2016-06-01-en

days of the request, unless there is an explicit request by the registrant or requestor to cancel the process, or the request verification was not successful.

Technical

On request and after verification, the Losing Registrar generates an AuthCode following best practices[46] and submits the AuthCode & TTL via EPP to the Registry System.

TTL : TBD (Best practise to be established)
EPP : <domain:update>

Until Registries have incorporated the TTL function into the protocol and their Registry Systems the Registrar should be responsible for setting a TTL in its own system adherence to a to-be-developed best practice.

Changes to standard

- New verification/notification requirement before issuance of AuthCode by Losing Registrar. No FOA2.
- A TTL is set for each Authcode in Registry System

Additional related steps not part of this process/policy

- Registrant removes transfer lock (if applicable)

3.2. Registrant authorizes domain name transfer

Flow

- Registrant orders domain name transfer with Gaining Registrar
- Registrant submits AuthCode to Gaining Registrar
- Gaining Registrar submits transfer request via EPP to Registry System
- Registry Operator checks and acknowledges transaction

[46] To be defined

Policy

Receiving an AuthCode is sufficient for the Gaining Registrar to initiate a transfer request.

Technical

Using standard EPP Transfer domain routine

EPP : <domain:transfer>
Syntax : as defined in RFC5731

Changes to standard

- No FOA1 Process for Gaining Registrar

3.3. Registry transfers the domain name

Flow

- Registry Operator checks Client Transfer Lock
- Registry Operator checks Server Transfer Lock
- Registry Operator checks AuthCode
- Registry Operator checks TTL
- Registry Operator notifies Gaining Registrar of transfer failure in case any check fails
- Registry Operator transfers domain object to Gaining Registrar
- Registry Operator notifies Gaining Registrar of transfer success in case no check fails
- Registry Operator notifies Losing Registrar of transfer success in case no check fails
- Registry Operator notifies Gaining Registrar of transfer of domain object
- Gaining Registrar updates domain object with new registrant data
- Gaining Registrar updates domain object with a new AuthCode, and sets TTL=Null

Policy

- Registry Operator needs to adhere to existing transfer policies[47] regarding lock status
- Registry Operator will transfer domain name immediately

[47] https://www.icann.org/resources/pages/registrars/transfers-en

- Registry Operator will not transfer any contact data with the domain object.

Technical

Using standard EPP transfer routine where possible

Until Registries have incorporated the TTL function into the protocol and their Registry Systems, Registries must not check the TTL.

Changes to standard

- Validity of the TTL must be processed
- Transfer must be processed immediately
- Transfer of domain object without contact data

Use cases and expected behavior regarding AuthCode

4.1. Registrant initiates transfer

- Losing Registrar sets new AuthCode & TTL at the Registry
- Losing Registrar informs the Registrant about AuthCode & TTL
- Losing Registrar does not store AuthCode token

4.2. Registrant lost AuthCode

- Losing Registrar sets new AuthCode & TTL at the Registry
- Losing Registrar informs the Registrant about AuthCode & TTL
- Losing Registrar does not store AuthCode

4.3. Registrant cancels transfer

- Losing Registrar updates domain object with a new AuthCode, and sets TTL=Null
- Losing Registrar does not store AuthCode

4.4. Transfer is processed and domain name is transferred to Gaining Registrar

- Registry Operator checks AuthCode & TTL
- Gaining Registrar updates domain object with registrant data
- Gaining Registrar sets new AuthCode and sets TTL=Null at Registry Level
- Gaining Registrar does not store the AuthCode

4.5. Transfer is requested but AuthCode is not correct

- Registry Operator denies the transfer. AuthCode stays as it is.

4.6. TTL of AuthCode expires without transfer being processed

- Registry Operator denies the transfer. AuthCode stays as it is.

ANNEX C Staff Report of Public Comment Proceeding

Preliminary Issue Report on a Policy Development Process to Review the Transfer Policy			
Publication Date:	14 December 2020		
Prepared By:	Caitlin Tubergen		
Public Comment Proceeding		Important Information Links	
Open Date:	12 October 2020	Announcement	
Close Date:	30 November 2020	Public Comment Proceeding	
Staff Report Due Date:	14 December 2020	View Comments Submitted	
Staff Contact:	Caitlin Tubergen	Email:	Policy-staff@icann.org
Section I: General Overview and Next Steps			

This Public Comment proceeding seeks to obtain community input on the Preliminary Issue Report on a Policy Development Process to Review the Transfer Policy.

Current Status: In accordance with the GNSO Policy Development Process (PDP) rules, ICANN org published the Preliminary Issue Report for Public Comment to allow for community input the Preliminary Issue Report. In particular, ICANN org sought specific input on the draft policy questions proposed in Section 3.5 of the Preliminary Issues Report, as well as the text provided in the draft Preliminary Charter in Annex A.

This Preliminary Issue Report on a Policy Development Process to Review the Transfer Policy examines, et.al, the issues identified in the Transfer Policy Initial Scoping Paper and includes:

a. Gaining & Losing Registrar Form of Authorization ("FOA")
b. Auth Code Management
c. Change of Registrant
d. Transfer Emergency Action Contact ("TEAC")
e. Transfer Dispute Resolution Policy ("TDRP")
f. Reversing/NACKing Transfers
g. ICANN-Approved Transfers
h. EPDP Rec. 27

Section 3 of the Preliminary Issues Report explores the above-referenced issues individually and provides references to documents and processes that could inform future policy work.

Next Steps: Following careful review of the public comments received, ICANN org will update the Preliminary Issue Report and submit a summary of the comments received together with the Final Issue Report to the GNSO Council for its consideration and potential action.

Section II: Contributors

At the time this report was prepared, a total of three (3) community submissions had been posted to the forum. The contributors, both individuals and organizations/groups, are listed below in chronological order by posting date with initials noted. To the extent that quotations are used in the foregoing narrative (Section III), such citations will reference the contributor's initials. Organizations and Groups:

Name	Submitted by
Hosting Concepts B.V. d/b/a Openprovider	Siemen Roorda
Tucows	Sarah Wyld
Registrar Stakeholder Group	Zoe Bonython

Section III: Summary of Comments

General Disclaimer: This section intends to summarize broadly and comprehensively the comments submitted to this public comment proceeding but does not address every specific position stated by each contributor. The preparer recommends that readers interested in specific aspects of any of the summarized comments, or the full context of others, refer directly to the specific contributions at the link referenced above (View Comments Submitted).

The three commenters, Openprovider, Tucows, and the Registrar Stakeholder Group all supported the topics identified in Preliminary Issue Report, noting all topics identified should be further considered by the eventual Working Group. Namely, the commenters supported the Working Group reviewing:

a. Gaining & Losing Registrar Form of Authorization ("FOA")
b. Auth Code Management
c. Change of Registrant
d. Transfer Emergency Action Contact ("TEAC")
e. Transfer Dispute Resolution Policy ("TDRP")
f. Reversing/NACKing Transfers
g. ICANN-Approved Transfers
h. EPDP Rec. 27

The substantive feedback received on each of the above topics is summarized below.

Gaining and Losing Registrar Form of Authorization ("FOA")

Openprovider noted the Gaining FOA is no longer necessary as it complicates the transfer process, particularly for registrars who operate under the wholesale model. Openprovider went on to note, "[w]e experience far lower [inter-registrar transfer] failure rates since the Temporary Specification allowed us to abandon the Gaining FOA in most cases. At the same time, we have not noticed any change in illegally transferred domain names because of abandoning the Gaining FOA."

Openprovider also noted the Losing FOA requirement should be removed, opting instead for a "transferred out notification". Openprovider suggested the notification instead of the FOA because the five-day waiting period is confusing for many registrants. Changing the FOA into a required notification allows the registrant to be informed of the transfer but prevents the delay, confusion, and associated frustration caused by the Losing FOA. Openprovider also

noted there should be a clear process for auditing and reversing an inter-registrar transfer in the event of a complaint.

Tucows noted that Question A1 in the "Gaining Registrar FOA and Losing Registrar FOA" section of the Preliminary Issues Report is confusingly worded because the second part of the question is based on a yes/no response to the first part of the question, and the first part of the question is not a yes/no question.

AuthInfo Codes

Openprovider commented that, given the growing value and importance of domain names, the AuthInfo process should be reviewed. In particular, it may be prudent for the eventual working group to consider additional security features for the AuthInfo code, such as a required minimum syntax and a limited validity period.

Openprovider additionally noted that (1) AuthInfo codes provide a sufficient paper trail for compliance auditing purposes, since many ccTLD registries rely exclusively on AuthInfo codes, (2) the current five-day service level agreement (SLA) for registrar provision of the AuthInfo code is appropriate, (3) the AuthInfo Code should be valid for 14-30 days and should be set by the registry, and (4) there should be a standard process through which a registrant can get the AuthInfo from the registry directly, without involvement of the current registrar since sometimes a losing registrar is uncooperative or out of business.

Change of Registrant

Openprovider noted the original goal of implementing Change of Registrant requirements was to protect domain name registrants against unauthorized changes to their domain name accounts; however, many registrars implemented a designated agent to auto-approve the change for both the previous and new registrant. Openprovider suggests a simple notification to the previous and new registrant, together with clear policies to review and revert unauthorized changes, should be sufficient. Lastly, Openprovider suggested "no locks, no opt-ins or opt-outs, no confirmations, no designated agents."

ICANN-Approved Transfers

All three commenters noted the topic of ICANN-approved transfers should be further explored by the eventual working group. Specifically, Openprovider noted, "the current scope of ICANN-Approved Transfers is restricted to 'all registrations' and it is restricted to 'acquisition' of the registrar or its assets, 'lack of accreditation' and lack of authorization with the Registry Operator. [. . .]. [W]e urgently request ICANN to develop a policy that allows for easier and faster voluntary bulk transfers between two registrars, similar to what many ccTLD registries already offer. At this moment, registrants and resellers that want to move their domain portfolio to another registrar are hindered by the bureaucratic processes, high fees, lack of standardization and lack of registry's cooperation. [. . .] [W]e consider the current policy contrary to the registrants' benefits and contrary to the above-cited text from §1.1. In other words: it strongly limits competition and free trade." Openprovider went on to suggest a

proposed voluntary bulk transfer process wherein the gaining and losing registrar could be free to reach a mutual agreement regarding the terms of the partial or full transfer, and the registry operator would be free to define the price for such transfer. In other words, the price for such transfer would not be mandated by an ICANN consensus policy.

Tucows also expressed a desire for the eventual working group to review the policy language for ICANN-approved transfers, noting "bulk transfers between registrars should be added to the list of topics which this Working Group is chartered to address. Policy which supports transferring domains in bulk at this time is limited to the BTAPPA process, which does not apply in most scenarios; as such, registrars and registrants would benefit from a more universal policy not tied to an acquisition." The Registrar Stakeholder Group went on to note, "although some registry operators utilize Bulk Transfer After Partial Portfolio Acquisition (BTAPPA), in order to provide this service, registry operators must first add it as an additional registry service through the Registry Services Evaluation Policy (RSEP). Because of these complicating factors, there may be differences between registry operators for bulk transfers, and not all registry operators may offer bulk transfers. The standardization of the bulk transfer process between registrars would allow registrars who are also acting as resellers to more efficiently consolidate their domains under management onto a single IANA credential, should they so desire. It may also harmonize divergent processes between registries, adding transparency and efficiency to the DNS ecosystem."

Working Group Model

Tucows noted it is open to using the "member/alternate/observer" model for the eventual Transfer Policy Working Group (as described in the draft charter), provided the membership model be included in the eventual PDP review process to evaluate the efficacy of this model.

Section IV: Analysis of Comments

General Disclaimer: This section intends to provide an analysis and evaluation of the comments submitted along with explanations regarding the basis for any recommendations provided within the analysis.

ICANN org staff thanks the commenters for the detailed feedback on the Preliminary Issue Report.

Policy Support Staff will be incorporating the above feedback related to the draft charter topics and text of the charter questions into the updated draft charter, which will be forwarded to the GNSO Council for its consideration. With respect to the substantive answers received in response to the draft charter questions, Policy Support Staff will provide this feedback to the eventual working group for its consideration.