

Initial Report on the Transfer Policy Review Policy Development Process

Status of This Document

This is the Initial Report of the GNSO Transfer Policy Review Policy Development Process Working Group that has been posted for public comment.

Preamble

The objective of this Initial Report is to document the working group's (i) deliberations on charter questions, (ii) preliminary recommendations, and (iii) additional identified issues to consider before the working group issues its Final Report.

Readers may notice this Initial Report differs in structure from a standard GNSO Initial Report. The differences are described below in the Prologue, but the structural reformatting ultimately aims to make the report more digestible and reader friendly.

After the working group reviews public comments received in response to this report, the working group will submit its Final Report to the GNSO Council for its consideration. In previous work, the working group submitted a prior initial report and public comment in June 2022.

Table of Contents

Table of Contents	2
Prologue	3
Overview of Recommendation Groupings	6
Policy Recommendations and Impact Analysis - Group 1(a)	7
Policy Recommendations and Impact Analysis - Group 1(b)	38
Policy Recommendations and Impact Analysis - Group 2	45
Annex 1 – Original Working Draft Recommendation Order	62
Annex 2 – Group 1(a) Charter Questions and WG Summary Deliberations	63
Annex 3 – Group 1(b) Charter Questions and WG Summary Deliberations	85
Annex 4 – Group 2 Charter Questions and WG Summary Deliberations	98
Annex 5 – Working Group Approach	116
Annex 6 – Working Group Membership and Attendance	120
Annex 7 – Community Input	125
Annex 8 – EPDP Phase 1, Rec. 27, Wave 1 Analysis	126
Annex 9 – Draft Edits to Transfer Dispute Resolution Policy (EPDP Rec. 27)	135
Annex 10 – Draft edits to Section I.B.1 of the Transfer Policy (Bulk Transfers)	146
Annex 11 – Additional Topics Discussed	148
Annex 12 – Group 1A Swimlane	151

Prologue

The Initial Report serves as a formal record of the Working Group’s work, discussions, proposed recommendations, and outstanding questions for the ICANN community. The Transfer Policy Review Working Group began its work in 2021; the past 3.5 years have included numerous discussions, agreements, and disagreements, which the Working Group has documented thoroughly within this report.

As readers may imagine, however, three years of discussions equates to a very long report, and the first iteration of the Initial Report, which was populated in the standard GNSO template, included over 100 pages of deliberations and recommendations, making it difficult for any reader to digest and respond within the time allotted during a standard public comment period of forty (40) days. The Working Group noted this potential difficulty and is publishing this Initial Report with a few important structural changes described below.

1. This **prologue** has been added to explain the changes to the standard Initial Report format.
 2. The opening **executive summary** has been replaced by three shorter summaries before each grouping of recommendations, in an effort to make the distinct topics from the policy recommendation groups, i.e., Group 1A, 1B, and 2 more understandable.
 3. The main body of the report includes a **table for each policy recommendation**, which includes:
 - a. **Recommendation # & Title**
 - b. **Recommendation Text:** the specific consensus recommendations proposed by the WG.
 - c. **Policy Impact Indicator:** a new feature to help the reader understand the degree of change being proposed by the Working Group, i.e., how much does this recommendation differ from the current Transfer Policy.
 - d. **Recommendation Rationale:** an explanation provided by the Working Group to explain and justify the proposed recommendation.
 - e. **Implementation Guidance:** where applicable, the Working Group included a brief explanation to assist in the implementation phase of the policy recommendations.
 - f. **Links to Charter Questions & Summary Deliberations:** The extensive summary deliberations and charter questions are now included in an annex to the report, which significantly reduces the length of the Initial Report body but allows interested readers who desire further historical context to easily toggle between the recommendation’s tables and the annex where the deliberations can be found.
-

Lastly, for the avoidance of doubt, the Policy Impact Indicator, Recommendation Rationale, Implementation Guidance, and the Linked Summary Deliberations are neither binding nor authoritative. These have been provided as supplementary text in an effort to help readers understand the context of the policy recommendations. Only the policy recommendation text itself is meant to be considered authoritative.

POLICY IMPACT ASSESSMENT (NEW feature)

In addition to developing, at a minimum, an Initial Report and Final Report detailing the Working Group's responses to its charter questions and accompanying policy recommendations, the Working Group is required to conduct and deliver a policy impact analysis. Specifically, the Working Group's [charter](#) provides, "If the WG concludes with any recommendations, the WG shall (or recommend the subsequent policy Implementation Review Team to) conduct a policy impact analysis." Historically, the impact analysis was left to the Implementation Review Team, a group that generally serves as an advisory body to ICANN org as ICANN org works to update an existing policy or creates a new policy, depending on the respective working group's recommendations, and inadvertently neglects to conduct this analysis.

Recognizing the importance of this analysis, this updated format of this report is an effort to provide a policy impact analysis, which is designed to indicate how much the recommendation differs from the status quo, or existing Transfer Policy. The policy impact assessment first includes a policy impact level, or the degree (low, medium, high) that the Working Group has used to indicate the degree of change the specific policy recommendation introduces.

"Policy Impact Level" (Low, Medium, High)

- An example of a **LOW** impact represents a small degree of change such as a definitional change rather than a substantive change to policy requirements, e.g., "Change of Registrant" to "Change of Registrant Data."
- An example of a **MEDIUM** impact represents a substantive change to the policy, such as a change to an existing requirement or the inclusion of a new requirement.
- An example of a **HIGH** impact would be a significant change to the current policy, such as the removal of a previous policy requirement, or the removal of the Post Change of Registrant 60-day transfer restriction.

When reviewing the policy impact level, it is important to note that the designated level is not a qualitative analysis of the policy recommendation. In other words, a recommendation classified as HIGH IMPACT does not mean the recommendation is bad or negative. Similarly, a recommendation classified as LOW IMPACT does not mean the recommendation is good or positive.

When considering the policy impact levels, the Working Group used the following non-exhaustive criteria:

- *Degree of change from existing requirement, e.g., no change or confirmation of existing requirement, modification to existing requirement, or new requirement)*
- *Security enhancement or removal of existing security requirement*
- *Level of technical change and corresponding impact to Contracted Parties*
- *ICANN Contractual Compliance enforcement capability*
- *Impact to Registered Name Holders (such as increased or reduced protections; level of confusion)*

This report contains many acronyms. The Working Group endeavored to include the meaning of the specific acronym when it first appears in the report; however, readers are invited to refer to ICANN's Acronyms and Terms page for unfamiliar acronyms: <https://www.icann.org/en/icann-acronyms-and-terms>.

Overview of Recommendation Groupings

Short Overview of Recommendation Grouping

The Working Group's [charter](#) divided the policy work into three distinct phases in recognition of the distinct topic areas and the significant time associated with each topic area.

- **Group 1(a):** Form of Authorization (including EPDP Phase 1, Recommendation 27, Wave 1 FOA issues), AuthInfo Codes, Denying (NACKing) transfers,
- **Group 1(b):** Change of Registrant (including EPDP Phase 1, Recommendation 27, Wave 1 Change of Registrant issues)
- **Group 2:** Transfer Emergency Action Contact and reversing inter-Registrar transfers, Transfer Dispute Resolution Policy (including EPDP Phase 1, Recommendation 27, Wave 1 TDRP issues), ICANN-approved transfers

Each group of recommendations will include an introduction to provide a high-level overview of the topic area before proceeding to the tables for each policy recommendation.

Lastly, the Working Group considers these recommendations to be interdependent, and, as a result, recommends the recommendations be considered as one package by the GNSO Council and subsequently the ICANN Board.

Policy Recommendations and Impact Analysis - Group 1(a)

Introduction to Group 1(a) Recommendations:

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.

The Group 1(a) recommendations cover many of the technical aspects of an inter-Registrar transfer, including, et al., the Gaining and Losing Form of Authorization, the Auth-Info Code, and other notifications associated with inter-Registrar transfers.

The ordering of the Group 1(a) recommendations corresponds to the approximate steps of an inter-Registrar transfer, which are visually depicted in the swimlane graph below. Within the diagram, there is a label for the corresponding recommendation number; however, please note that not all steps of the diagram contain a recommendation number.

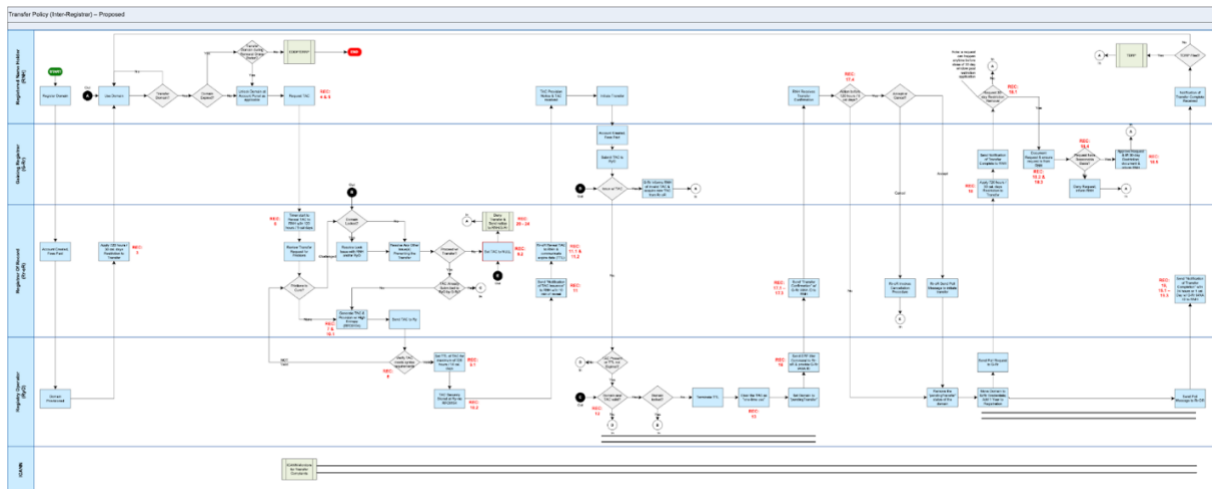
In order to synchronize the recommendation numbers with the swimlane graph, the previous numbering from the first Initial Report has been changed. The original Initial Report numbering corresponded to the order of the charter questions, and the previous recommendation ordering can be found in this [annex](#).

Disclaimers about the swimlane:

1. The swimlane is a conceptual representation of the proposed transfer process and serves as a guide to assist readers in understanding the proposed Group 1A recommendations. The swimlane is NOT a policy requirements document, and, accordingly, should not be treated as such.
2. The swimlane is constructed at a very high-level. It does not account for all variations of possible transfer transactions, especially considering the varying business models and procedures across contracted parties.
3. Where a process step box does not have a recommendation label, it is NOT specific to any proposed recommendation or a policy requirement. These process steps are only used to maintain logical continuity of a transfer transaction from beginning to end.

- 4. A deficiency of the swimlane model is it does NOT accurately represent time scales. This conceptual model blends system processes that occur in seconds vs. business procedures that could occur over several calendar days.

The following diagram is presented only as a reference to its existence, please refer to this [link](#) for a more consumable version of the swimlane or you can find an embedded version in the last [annex](#) of this report.



Recommendation #1: Terminology Updates: Whois

The working group recommends the following specific terminology updates to the Transfer Policy and the Transfer Dispute Resolution Policy:

- (i) The term "Whois data" SHALL have the same meaning as "Registration Data".
- (ii) The term "Whois details" SHALL have the same meaning as "Registration Data".
- (iii) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".
- (iv) The term "Whois" SHALL have the same meaning as "RDDS".

For the avoidance of doubt, the terms referenced in above in Recommendation 1 (i) - (iv) are intended to correspond to the definitions in the Registry Agreement ("RA") and the Registrar Accreditation Agreement ("RAA"), as appropriate. In the event of any inconsistency, the RA/RAA definitions, if updated, will supersede. The working group also recommends that the outdated terms should be replaced with the updated terms, e.g., all references to "Whois Data" should be replaced with the term "Registration Data," etc.

Policy Impact:

LOW - Terminology changes only.

Recommendation Rationale:

This recommendation is consistent with the EPDP Team's Phase 1 Recommendation 24. The working group additionally notes that for purposes of the Transfer Policy, Registration Data means the contact data collected by a Registrar from a legal or natural person in conjunction with the registration of a domain name. It is not meant to include additional customer data such as credit card details and email correspondence.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[c1](#), [c2](#), [j1](#)

Recommendation #2: Terminology Updates: Administrative Contact and Transfer Contact

The working group recommends removing any reference to an “Administrative Contact” or “Transfer Contact” in the Transfer Policy and Transfer Dispute Resolution Policy and replacing it with “Registered Name Holder” unless specifically indicated.

Policy Impact:

LOW - Terminology changes only.

Recommendation Rationale:

Under the upcoming Registration Data Policy, Administrative Contact data is no longer required to be collected by the Registrar, and therefore cannot be relied upon for Transfer Policy requirements. Accordingly, the Registered Name Holder would be the only authorized transfer contact.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[c1](#), [c2](#), [j1](#)

Recommendation #3: Transfer Restriction After Initial Registration

The Registrar **MUST** restrict the RNH from transferring a domain name to a new Registrar within 30 calendar days / 720 hours of the initial registration date.¹ To the extent that a Registry and/or Registrar has an existing policy and/or practice of restricting the RNH from transferring a domain name to a new Registrar for a different period of time following initial registration, all policies and practices **MUST** be updated to be consistent with this new requirement.²

¹ The initial registration date referenced in this recommendation corresponds to the Creation Date in the RDDS.

² For the avoidance of doubt, this includes, but is not limited to, a 60-day post-creation lock currently specified in some Registry-Registrar Agreements (RRAs). Recommendation 3 seeks to standardize the inter-Registrar transfer restriction period to 30 days across all gTLDs. Accordingly, an RRA or registration agreement that specifies a period other than 30 days would need to be amended pursuant to this recommendation, as a 60-day post-creation lock (or period other than 30 days) would no longer be permitted under the Transfer Policy.

Policy Impact:

LOW - Restriction changed from an inconsistent use of 60 days, via Registry-Registrar agreements to a consistent use of 30 calendar days/ 720 hours as part of a Consensus Policy recommendation.

Recommendation Rationale:

The working group believes that a single requirement across the industry will result in a better experience for registrants. The working group recommends that 30 days is the appropriate period for this requirement because:

- It provides a window of opportunity to identify issues associated with credit card payments, including unauthorized use of a credit card. This may assist with addressing criminal activity and deterring fraud.
- It provides a window of opportunity for a complainant to file a Uniform Domain Name Dispute Resolution Policy (UDRP) proceeding without the domain being transferred to a new Registrar. Once the proceeding is underway, the domain will be locked in relation to the dispute.
- For registrants who legitimately want to transfer a domain shortly after registration, the working group believes that 30 days is a reasonable period of time to wait.

To clarify, use of the term “lock” is not intended to imply or require a specific technical solution for implementation. Rather, it is used as shorthand meaning that the domain is ineligible for inter-Registrar transfer for a period of time.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

This recommendation does not have a direct link to any charter question as this issue only surfaced through further analysis of transfer “locks” being applied at different stages of the domain lifecycle.

Recommendation #4: Update Term “AuthInfo Code” to “Transfer Authorization Code (TAC)”

The working group recommends that the Transfer Policy and all related policies MUST use the term “Transfer Authorization Code” or “TAC” in place of the currently used term “AuthInfo Code” and related terms. This recommendation is for an update to terminology only and does not imply any other changes to the substance of the policies.

Policy Impact:

LOW - Terminology changes only.

Recommendation Rationale:

The working group believes it is clearer for all parties, and particularly the Registered Name Holder, if a single term is used universally. “Transfer Authorization Code” (TAC) provides a straightforward description of the code’s function.

Implementation Guidance:

ICANN’s publications and webpages should also be updated to reflect the recommended terminology change described in Recommendation 4.

Links to Charter Question(s) & Summary of Deliberations:

[b1](#)

Recommendation #5: TAC Definition

The working group recommends that the Transfer Authorization Code MUST be defined as follows: “A Transfer Authorization Code (TAC) is a token created by the Registrar of Record and provided upon request to the RNH or their designated representative. The TAC is required for a domain name to be transferred from one Registrar to another Registrar and when presented authorizes the transfer.”³ Relevant policy language MUST be updated to be consistent with this definition.

- “Designated representative” means an individual or entity that the Registered Name Holder explicitly authorizes to request and obtain the TAC on their behalf. In the event of a dispute, the RNH’s authority supersedes that of the designated representative.

³ Note: This definition draws on elements included in Recommendation 10.

Policy Impact:

LOW - Clarification of definition.

Recommendation Rationale:

This definition is a revision of a text included on the [ICANN.org](https://www.icann.org) website, updated to make clear that the TAC's function is to verify that the Registered Name Holder (RNH) requesting the transfer is the same RNH who holds the domain. For the avoidance of doubt, the term "designated representative" introduced by the working group in Recommendation 5 is distinct from the concept of a "designated agent," which is defined in Transfer Policy Section I.A.1.2.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[b1](#)

Recommendation #6: Service Level Agreement (SLA) for TAC Provision

The working group confirms that the Transfer Policy MUST continue to require the Registrar to set the TAC at the Registry and issue the TAC to the RNH or their designated representative within five calendar days of a request, although the working group recommends that the policy state the requirement as 5 calendar days/120 hours rather than 5 calendar days to reduce any risk of confusion. The working group further recommends that the policy MUST make clear that 5 calendar days/120 hours is the maximum and not the standard period in which the TAC is to be issued.

Policy Impact:

LOW - Clarification of status quo.

Recommendation Rationale:

The working group did not identify a compelling reason to change the five-day response time frame but believes that it is clearer to express the time frame in both hours and calendar days. In updating the timing, the working group also wished to make clear that 5 calendar days/120 hours is the maximum time rather than the standard time in which the TAC is to be issued. This highlights that quicker turnaround time is possible and desirable in many cases.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[b3](#)

Recommendation #7: TAC Composition

The working group recommends that the minimum requirements for the composition of a TAC MUST be as specified in RFC 9154, including all successor standards, modifications or additions thereto relating to Secure Authorization Information for Transfer. The requirement in section 4.1 of RFC 9154 regarding the minimum bits of entropy (i.e., 128 bits) should be a MUST in the policy until a future RFC approved as “Internet Standards” (as opposed to Informational or Experimental standards) through the applicable IETF processes updates the security recommendation.

Policy Impact:

MEDIUM - Updated security requirements to the TAC will involve planning and system changes for Registrars and enhanced security for registrants.

Recommendation Rationale:

The working group supports the statement in RFC 9154 section 4.1 that “For authorization information to be secure, it MUST be generated using a secure random value.”

Recommendation 7 brings requirements for the composition of the TAC in line with RFC 9154, including all successor standards, modifications or additions thereto relating to Secure Authorization Information for Transfer.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[a4](#), [b2](#)

Recommendation #8: Verification of TAC Composition

The working group recommends that, at the time that the TAC is stored in the Registry system, the Registry MUST verify that the TAC meets the syntax requirements specified in Recommendation 7.

Policy Impact:

MEDIUM - New requirements for Registries will require planning and system changes.

Recommendation Rationale:

Registry verification provides a check on the randomness of the authorization information generated by the Registrar.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[a4](#), [b2](#)

Recommendation #9: TAC Time to Live (TTL)

The working group recommends that:

9.1: The TAC MUST be valid for 14 calendar days / 336 hours from the time it is set at the Registry, enforced by the Registry.

9.2: The Registrar of Record MAY reset the TAC to null⁴ prior to the end of the 14th calendar day / 336 hours by agreement by the Registrar of Record and the RNH.

Policy Impact:

MEDIUM - New requirements for both Registries and Registrars will require planning and system changes.

⁴ In the context of this recommendation, “reset the TAC to null” is to have the opposite meaning of setting the TAC. In other words, Recommendation 10.2 provides that the Registrar of Record sets the TAC at the Registry; here, the Registry is reversing that action.

Recommendation Rationale:

The purpose of the standard Time to Live (TTL) is to enforce security around unused TACs (e.g., requested/received but not used), in a situation where the TAC may be stored in a registrant's email or other communications storage. The working group arrived at the conclusion that the TAC TTL must be no more than 14 calendar days / 336 hours and notes that a 14-day / 336 hour period is appropriate in order to accommodate transfer-related business processes associated with different Registrar models.

The working group extensively discussed whether the Registry or Registrar should enforce the 14-day TTL and requested community input on this question through public comment on the Phase 1A Initial Report. The working group recommends enforcement by the Registry for the following reasons:

- For accuracy: If the sponsoring Registrar is required to expire the TAC by updating it to null, there is a possibility that at the time when the TAC is set to expire, either the Registrar or Registry systems have an outage (or there is a communication interruption). This means that the TAC expiration would be delayed until the transaction could be completed, opening a window for possible usage of a TAC that the sponsoring Registrar had deemed expired.
- For consistency: Having a centralized approach at the Registry allows the prospective Gaining Registrar to know that every TAC will expire at 14 days / 336 hours regardless of the sponsoring/provisioning Registrar's location or timezone.
- For security: Every TAC in a Registry has a maximum lifetime that is enforced consistently. This prevents the existence of any long-lived TAC, which could be used as part of an unauthorized or unintended inter-Registrar transfer.

With respect to 9.2, the working group acknowledged that there may be a variety of circumstances in which the Registrar of Record and the Registered Name Holder may want to mutually agree to reset the TAC to NULL prior to the end of the 14th calendar day. The working group included this language to ensure that the Registrar of Record is permitted to do so under relevant circumstances.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[b4](#)

Recommendation #10: TAC Generation, Storage, and Provision

The working group recommends that:

10.1: The TAC MUST only be generated by the Registrar of Record upon request by the RNH or their designated representative.

10.2: When the Registrar of Record sets the TAC at the Registry, the Registry MUST store the TAC securely, at least according to the minimum standard set forth in RFC 9154 (or its successors).

Policy Impact:

MEDIUM - Recommendation adds new TAC security requirements for both Registrars and Registries and will involve planning and system changes.

Recommendation Rationale:

Currently, it can be the case that a TAC exists and is stored over an extended period of time and therefore can be at risk of breach or theft, for example at the Registrar of Record or via an RNH's email account. This recommendation seeks to reduce the risk of unintended disclosure of the TAC by ensuring that the TAC is only generated at the point that it is needed to initiate an inter-Registrar transfer, reducing the risk of the TAC getting in the wrong hands once it is generated (Recommendation 10.1). This recommendation further protects against breach or theft at the Registry by ensuring that the Registry stores the TAC in a secure manner (Recommendation 10.2).

Implementation Guidance:

RFC 9154 recommends using a strong one-way cryptographic hash with at least a 256-bit hash function, such as SHA-256 [FIPS-180-4], and with a per-authorization information random salt with at least 128 bits.⁵

Links to Charter Question(s) & Summary of Deliberations:

[a4](#)

⁵ [FIPS-180-4] National Institute of Standards and Technology, U.S. Department of Commerce, "Secure Hash Standard, NIST Federal Information Processing Standards (FIPS) Publication 180-4", DOI10.6028/NIST.FIPS.180-4, August 2015, <<https://csrc.nist.gov/publications/detail/fips/180/4/final>>.

Recommendation #11: Notification of TAC Issuance

The working group recommends that the Registrar of Record MUST send a “Notification of TAC Issuance”⁶ to the RNH without undue delay but no later than 10 minutes after the Registrar of Record issues the TAC.⁷ For the purposes of sending the notification, the Registrar of Record MUST use contact information as it was in the registration data at the time of the TAC request.

11.1: This notification MUST be provided in English and in the language of the registration agreement and MAY also be provided in other languages.

11.2: The following elements MUST be included in the “Notification of TAC Issuance”:

- Domain name(s)
- Explanation that the TAC will enable the transfer of the domain name to another Registrar
- Date and time that the TAC was issued and information about when the TAC will expire
- Instructions detailing how the RNH can take action if the request is invalid (how to invalidate the TAC)
- If the TAC has not been issued via another method of communication, this communication will include the TAC

Policy Impact:

MEDIUM - This recommendation requires a new notification. Implementation of this feature will require planning and system updates for Registrars, and the RNH will experience changes from the current transfer policy.

Recommendation Rationale:

This recommendation seeks to ensure that the RNH consistently receives the necessary information with respect to an inter-Registrar transfer. If the RNH receives the notice and determines that the action on the account is unauthorized or unintended, the RNH may seek to

⁶ The working group recognizes that this notification MAY be sent via email, SMS, or a secure messaging system determined by the Registrar. These examples are not intended to be limiting, and it is understood that additional methods of notification MAY be created that were not originally anticipated by the working group.

⁷ The working group recognizes that from a security perspective, it is best for the “Notification of TAC Issuance” to be delivered by a method of communication that is different from the method used to deliver the TAC. If this is not possible, and the same method of communication is used, the Registrar of Record MAY choose to send the “Notification of TAC Issuance” and the TAC together in a single communication.

invalidate the TAC before the transfer completes. The working group has recommended additional security enhancements to the inter-Registrar transfer process, including these changes to the TAC, in recognition of the removal of the Gaining FOA and the importance of ensuring inter-Registrar transfers remain secure under the new domain name landscape. Additional details regarding the working group's thinking can be found in the discussions section of Annex 2.

Implementation Guidance:

In cases where a customer uses a Privacy/Proxy service and the contact information associated with the underlying customer is known to the Registrar of Record, the Registrar of Record MAY send the notification directly to the underlying customer.

Links to Charter Question(s) & Summary of Deliberations:

[a4](#), [a7](#), [a8](#)

Recommendation #12: Verification of TAC Validity

The working group recommends that Registry Operator MUST verify that the TAC provided by the Gaining Registrar is valid in order to accept an inter-Registrar transfer request.

Policy Impact:

LOW - This recommendation confirms the status quo under the Temporary Specification, i.e., no significant change is involved.

Recommendation Rationale:

This recommendation is consistent with Appendix G: Supplemental Procedures to the Transfer Policy contained in the Temporary Specification for gTLD Registration Data.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[b2](#)

Recommendation #13: TAC is One-Time Use

The working group recommends that the TAC as created by the Registrar of Record according to Recommendation 10 MUST be “one-time use.” In other words, it MUST be used no more than once per domain name. The Registry Operator MUST reset the TAC to null⁸ when it accepts a valid TAC from the Gaining Registrar.

Policy Impact:

MEDIUM - New requirements for Registrars will involve planning and system changes.

Recommendation Rationale:

The one-time use principle limits the number of transactions that can be completed using a single password to one, reducing the damage that can be caused by a bad actor. The working group believes that it is good practice to manage the TAC following the one-time use principle.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[b1](#)

Recommendation #14: Maintenance of Records

The Registrar MUST retain all records pertaining to the provision of the Transfer Authorization Code (TAC)⁹ to a Registered Name Holder, as well as all notifications sent per the requirements under the Transfer Policy. At a minimum, the records retained MUST document the date/time, means, and contact(s) to whom the TAC and notifications are sent. The Registrar MUST maintain these records for the shorter of 15 months or the longest period permitted by applicable law, and during such period MUST provide such records to ICANN upon reasonable notice.

⁸ In the context of this recommendation, “reset the TAC to null” is to have the opposite meaning of setting the TAC. In other words, Recommendation 10.2 provides that the Registrar of Record sets the TAC at the Registry; here, the Registry is reversing that action.

⁹ Details about the Transfer Authorization Code (TAC) are discussed in earlier in this Report.

Policy Impact:

LOW - Registrars must already maintain relevant records; this recommendation seeks to make the retention period consistent with the Registration Data Policy, because it also processes personal data of the RNH.

Recommendation Rationale:

This recommendation seeks to ensure that the necessary information is available to ICANN org in the case of a Compliance investigation related to an inter-Registrar transfer. The 15-month retention period specified in this recommendation is consistent with requirements in the Registration Data Policy.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[a5](#)

Recommendation #15: Gaining Form of Authorization (FOA)

The working group recommends eliminating from the Transfer Policy the requirement that the Gaining Registrar send a Gaining Form of Authorization. This requirement is detailed in section 1.A.2 of the Transfer Policy.

Policy Impact:

LOW - Since the introduction of the Temporary Specification for gTLD Registration Data, compliance enforcement of the Gaining FOA has been placed on hold, and Registrars do not use the Gaining FOA to confirm transfers. Accordingly, this recommendation does not change the current practice.

Recommendation Rationale:

As discussed in detail in the working group's response to charter question a1, the inter-Registrar transfer process has functioned without the Gaining FOA since the GDPR went into force and the Temporary Specification modified ICANN obligations, and the working group has not encountered any evidence that there has been an increase in unauthorized transfers since the Gaining FOA was functionally eliminated. It has not found any other indications that the

transfer process is malfunctioning without the Gaining FOA requirement. Therefore, the working group sees no evidence that the Gaining FOA is needed for the purpose of facilitating the transfer or protecting the RNH from unauthorized transfers.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[a1](#), [j1](#)

Recommendation #16: Registry Transmission of IANA ID to Losing Registrar

The Registry Operator MUST provide the Gaining Registrar's IANA ID to the Losing Registrar in the notification of a pending transfer request, which will enable the Losing Registrar to provide this information in the Transfer Confirmation and Notification of Transfer Completion.

Policy Impact:

MEDIUM - This recommendation involves a new requirement for Registries, which will involve planning and system updates.

Recommendation Rationale:

Currently, not all Registry Operators use the Gaining Registrar's IANA ID when notifying a Losing Registrar of a pending transfer request. Instead, some Registry Operators use a separate, internal client ID that does not correspond to the IANA ID. This recommendation enables the Losing Registrar to consistently provide the IANA ID in the Transfer Confirmation and Notification of Transfer Completion. In the case of a legitimate transfer, this information allows the RNH to confirm that the desired action was completed as requested. If the transfer is not consistent with the RNH's intent, the IANA ID is an important data point to assist the RNH with investigating the issue.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[a7](#)

Recommendation #17: Losing Form of Authorization (FOA)

The working group did not reach agreement to eliminate or substantially change the Obligations of the Registrar of Record described in Section I.A.3.1 - I.A.3.6 of the Transfer Policy. Therefore, the working group recommends that these requirements will largely remain in place. The working group recommends the following minor modifications:

17.1: The term “Transfer Confirmation” MUST be used in place of “Standardized Form of Authorization (FOA).”

17.2: The Transfer Confirmation language MUST include the Gaining Registrar’s IANA ID and a link to ICANN-maintained webpage listing accredited Registrars and corresponding IANA IDs. If available, the name of the Gaining Registrar MAY also be included.

17.3: The Transfer Confirmation MUST be provided in English and the language of the registration agreement and MAY also be provided in other languages.

17.4: The timeframe of five (5) calendar days specified in section I.A.3.5 of the policy MUST be expressed in both calendar days and hours: “Failure by the Registrar of Record to respond within five (5) calendar days / 120 hours to a notification from the Registry regarding a transfer request will result in a default "approval" of the transfer.”

Policy Impact:

LOW - Status quo largely remains unchanged.

Recommendation Rationale:

Please see response to charter question a7 for a summary of the working group’s deliberations on the Transfer Confirmation. Regarding the minor modifications recommended by the working group:

- The term “Losing Form of Authorization” may be confusing to the RNH, and therefore the working group recommends an update in terminology to “Transfer Confirmation,” which more accurately describes the function that is served.
- With inclusion of the IANA ID in the Transfer Confirmation, the RNH can confirm that the Gaining Registrar matches the Registrar to whom the RNH intends to transfer to domain. If the pending transfer is not consistent with the RNH’s intent, the IANA ID is an important data point to assist the RNH with investigating the issue.

- Providing the Transfer Confirmation in English and the language of the registration agreement improves accessibility for the RNH.

Consistent with the other recommendations in this report, the working group recommends specifying timeframes in both calendar days and hours for greater clarity.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[a7](#)

Recommendation #18: Transfer Restriction After Inter-Registrar Transfer

The Registrar MUST restrict the RNH from transferring a domain name to a new Registrar within 30 calendar days / 720 hours of the completion of an inter-Registrar transfer. To the extent that a Registry and/or Registrar has an existing policy and/or practice of restricting the RNH from transferring a domain name to a new Registrar for a different period of time following an inter-Registrar transfer, all policies and practices MUST be updated to be consistent with this new requirement. However, the working group recognizes that there may be situations where early removal of the 30-day restriction described in Recommendation 18 is appropriate. Accordingly, the Registrar MAY remove the 30-day inter-Registrar transfer restriction early only if all of the below conditions are met:

18.1: The Registrar MUST be able to demonstrate that it received a specific request to remove the 30-day restriction from the Registered Name Holder;

18.2: The Registrar MUST ensure the request to remove the restriction was requested by the Registered Name Holder;

18.3: The specific request includes a reasonable basis for removal of the restriction; and

18.4: The Registrar MUST maintain a record demonstrating the request to remove the restriction (regardless of outcome) for a period of no fewer than fifteen (15) months following the end of the Registrar's sponsorship of the registration.

Policy Impact:

MEDIUM - New post-transfer restriction is reduced from an inconsistently-applied 60 days to a consistently-applied 30 days via Consensus Policy. NOTE: The working group discussed the mandatory 30-day post-inter-Registrar transfer restriction and noted the mandatory restriction gave the group more comfort with the inability to send the Gaining FOA and other previous security features.

Recommendation Rationale:

The working group believes that a single requirement across the industry will result in a better experience for registrants and will also consistently prevent the transfer of a domain multiple times in rapid succession, a practice associated with domain theft. The working group recommends that 30 days is the appropriate period for this requirement because:

- It provides a window of opportunity to identify issues associated with credit card payments, including unauthorized use of a credit card. This may assist with addressing criminal activity and deterring fraud.
- For registrants who legitimately want to transfer a domain again shortly after an inter-Registrar transfer has taken place, 30 days is a reasonable period of time to wait.

Implementation Guidance:

The working group notes that the 30-day post-transfer restriction is an important security mechanism to prevent Registrar hopping and potential domain theft, however the working group also recognizes that there may be situations where early removal of the 30-day post-transfer restriction is necessary. Such situations identified by the working group may include, but are not limited to:

- Well informed, documented, clearly intentional request by the registrant
 - Mutual agreement between the prior and current Registrar of a transfer back to the prior Registrar
 - Legitimate circumstances surrounding an escrow intermediary affecting the completion of the acquisition of the involved registered domain name
 - To complete documented registered domain name acquisition (aftermarket purchase, portfolio consolidation, or bona fide purchase)
 - Intentional release of the registered domain name that had transferred to the Registrar where it becomes evident the domain name use would be in violation of the Registrar's Acceptable Use Policy (AuP), Terms of Service (ToS), or local law or other similar governance.
-

Links to Charter Question(s) & Summary of Deliberations:[a6](#), [h1](#)

Recommendation #19: Notification of Transfer Completion

The working group recommends that the Losing Registrar¹⁰ MUST send a “Notification of Transfer Completion”¹¹ to the RNH without undue delay but no later than 24 hours after the transfer is completed. For the purposes of sending the notification, the Losing Registrar MUST use contact information as it was in the registration data at the time of the transfer request.

19.1: This notification MUST be provided in English and in the language of the registration agreement and MAY also be provided in other languages.

19.2: To the extent that multiple domains have been transferred to the same Gaining Registrar or to multiple Gaining Registrars at the same time, and the RNH listed in the Registration Data at the time of the transfer is the same for all domains, the Registrar of Record MAY consolidate the “Notifications of Transfer Completion” into a single notification.

19.3: The following elements MUST be included in the “Notification of Transfer Completion”:

- Domain name(s)
- IANA ID(s) of Gaining Registrar(s) and link to ICANN-maintained webpage listing accredited Registrars and corresponding IANA IDs. If available, the name of the Gaining Registrar(s) may also be included.
- Text stating that the domain was transferred
- Date and time that the transfer was completed
- Instructions detailing how the RNH can contact the Losing (Prior) Registrar for support if they believe the transfer was invalid, and any deadlines or policies which may be relevant.

¹⁰ This is the Registrar of Record at the time of the transfer request.

¹¹ The footnote on Recommendation 11 regarding the method by which notifications are sent equally applies to the “Notification of Transfer Completion.”

Policy Impact:

MEDIUM - This recommendation requires a new notification, which will require planning and system updates for Registrars.

Recommendation Rationale:

This recommendation seeks to ensure that the RNH consistently receives the necessary information with respect to an inter-Registrar transfer. If the RNH receives the notice and determines that the transfer is unauthorized or unintended, the RNH may seek the appropriate remedy.

Implementation Guidance:

In cases where a customer uses a Privacy/Proxy service and the contact information associated with the underlying customer is known to the Registrar of Record, the Registrar of Record MAY send the notification directly to the underlying customer.

For this recommendation and others, the following definitions from the Transfer Dispute Resolution Policy reflect the accurate meaning of the terms referenced throughout this Initial Report:

Gaining Registrar: The Registrar who seeks to become the Registrar of Record by submitting a transfer request.

Losing Registrar: The Registrar who was the Registrar of Record at the time a request for the transfer of domain is submitted.

Registrar of Record:

The Registrar who sponsors a domain name at the registry.

Links to Charter Question(s) & Summary of Deliberations:

[a7](#), [a8](#)

Recommendation #20: Format of Transfer Policy Section I.A.3.7

I.A.3.7 of the Transfer Policy currently reads, “Upon denying a transfer request for any of the following reasons, the Registrar of Record must provide the Registered Name Holder and the potential Gaining Registrar with the reason for denial. The Registrar of Record MAY deny a transfer request only in the following specific instances:” The working group recommends the following revision, in bold, to the first sentence: “Upon denying a transfer request for any of the following reasons, the Registrar of Record must provide the Registered Name Holder and, **upon request**, the potential Gaining Registrar with the reason for denial.” The working group further recommends expressing the two sentences of this provision as two distinct provisions of the policy.

Policy Impact:

LOW - This recommendation is meant to clarify the status quo.

Recommendation Rationale:

The addition of the words “upon request” to the first sentence is intended to clarify that while the Registrar of Record always provides the reason for denial to the RNH, the Registrar of Record only provides the reason for denial to the Gaining Registrar upon request. There is no automated process to provide the reason for denial to the Gaining Registrar. This is currently the case and is expected to continue to be the case in the future. The two sentences of I.A.3.7 express two distinct concepts and therefore should be separated into two different provisions.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[h1](#)

Recommendation #21: Revised Reasons that a Registrar of Record MAY Deny a Transfer

The working group recommends revising the following reasons that the Registrar of Record **MAY** deny a transfer request as follows:

Reference	Current Text	Revision	Rationale
I.A.3.7.1	Evidence of fraud.	Evidence of (a) fraud or (b) DNS Abuse as defined in Section 3.18.1 of the Registrar Accreditation Agreement.	ICANN’s Contractual Compliance Department has observed difficulties from Registrars tying transfer denials involving domain names suspended for abusive activities to the denial instances contemplated by the Transfer Policy. The working group considered several possible revisions to I.A.3.7.1, including those submitted through public comment on the Phase 1(a) Initial Report, to appropriately address the issue identified while ensuring that the text is clear and narrowly-tailored. The working group wanted to avoid recommending broad language that might enable a Registrar to either a) prevent a transfer arbitrarily or b) prevent an RNH from transferring a domain from a jurisdiction where certain content or activity is illegal or restricted to another jurisdiction where that same content or activity is considered legitimate speech. The working group’s proposed revision seeks to strike this balance. The WG intentionally points to an ICANN-maintained webpage in the text to allow for changes in the specific threats that may be considered a DNS Security Threat in the ICANN context.
I.A.3.7.2	Reasonable dispute over the identity of the Registered Name Holder or Administrative Contact.	Reasonable dispute over the identity of concern that the transfer was not requested by the Registered Name Holder or Administrative Contact.	The working group believes that the term “identity” is not appropriate in this context, in part due to concerns regarding data privacy implications.

			<p>Because the issue at hand is more precisely about authority over the domain, the working group refined the text to focus on the key underlying concern, namely that the transfer request was made by a party other than the Registered Name Holder.</p> <p>Under the Registration Data Policy, Administrative Contact data is no longer collected by the Registrar, therefore this term has been removed. This update is consistent with Recommendation 15.</p> <p>The working group considered adding language to address other types of invalid requests or disputes by other parties. The working group determined that the use cases they discussed are appropriately covered by the revised language in I.A.3.7.2.</p>
<p>I.A.3.7.3</p>	<p>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.</p>	<p>Nonpayment for previous registration period (including payment disputes or credit card charge-backs) if the domain name is past its expiration date at the current Registrar of Record 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.</p>	<p>The working group has added the term "payment disputes" to reflect problems related to payments other than a credit card charge-back.</p> <p>The working group received input from ICANN's Contractual Compliance Department that the term "expiration date" in this provision is not sufficiently precise, because during the Auto-Renew Grace Period, the domain will not show as expired at the Registry level, but will show as expired at the Registrar of Record. By adding "at the current Registrar of Record" the working group has clarified that if the domain name is past its expiration date at the current Registrar of Record and the</p>

			<p>RNH has not paid for the registration period prior to that expiration date, the Registrar of Record may deny the transfer.</p> <p>The working group notes that the sentence beginning “In all such cases. . .” dates back as early as the 2002 ICANN DNSO Transfers Task Force Final Report & Recommendations.</p> <p>The working group believes that the Expired Registration Recovery Policy now provides the necessary guidance on treatment of domains post-expiration and that this sentence is unnecessary in the Transfer Policy text.</p>
--	--	--	--

Policy Impact:

LOW - Clarification of existing text.

Recommendation Rationale:

The working group reviewed the text and proposed the above edits for clarity. The rationale for the proposed changes is described within the table above.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[h1](#)

Recommendation #22: Revised Reasons that a Registrar of Record MUST Deny a Transfer

The working group recommends changing the following reasons that the Registrar of Record currently MAY deny a transfer into reasons that the Registrar of Record MUST deny a transfer and revising the text as follows:

Reference	Current Text	Revision	Rationale
I.A.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.	Express objection to the transfer by the authorized Transfer Contact Registered Name Holder . Objection could take the form of specific request (either by paper or electronic means) by the authorized Transfer Contact Registered Name Holder 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 Registered Name Holder on an opt-in basis and upon request by the authorized Transfer Contact Registered Name Holder , the Registrar must remove the lock or provide a reasonably accessible method for the authorized Transfer Contact Registered Name Holder to remove the lock within five (5) calendar days.	Under the Registration Data Policy, Administrative Contact data is no longer collected by the Registrar. Accordingly, the RNH would be the only authorized transfer contact. The working group believes that it is logical that the Registrar of Record must deny a transfer if the Registered Name Holder expressly objects to the transfer. This update is consistent with Recommendation 15.
I.A.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.	The transfer was requested within 60 30 days of the creation date as shown in the registry Whois RDDS record for the domain name.	Per working group Recommendation 3, the Registrar MUST restrict the RNH from transferring a domain name to a new Registrar within 30 days of the initial registration date. "Whois" has been updated to "RDDS" consistent with Recommendation 1.

<p>I.A.3.7.6</p>	<p>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.</p>	<p>A domain name is within 60-30 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. This restriction does not apply in cases where the conditions described in [policy references to be inserted] are met.</p>	<p>Per working group Recommendation 19, the Registrar MUST restrict the RNH from transferring a domain name to a new Registrar within 30 days of the completion of an inter-Registrar transfer, unless the conditions described in Rec. 18.1-18.4 are met.</p>
------------------	--	---	---

Policy Impact:

LOW - Textual changes for clarity and consistency with other policy recommendations in this report.

Recommendation Rationale:

The working group believes changing MAY to MUST allows for increased consistency across the industry and provides more predictability to registrants.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[h1](#)

Recommendation #23: Revised Reasons that a Registrar of Record MUST Deny a Transfer

The working group recommends revising the reasons that the Registrar of Record MUST deny a transfer request as follows:

Reference	Current Text	Revision	Rationale
I.A.3.8.1	A pending UDRP proceeding that the Registrar has been informed of.	A Pending UDRP proceeding that the Registrar has been informed notified of by the Provider in accordance with the UDRP Rules.	The working group has refined the current text in an effort to clarify that Registrars must deny inter-Registrar transfer requests that are received after a Registrar has been notified by a UDRP Provider of a UDRP proceeding in accordance with the UDRP Rules.
I.A.3.8.2	Court order by a court of competent jurisdiction.	N/A	The working group believes that this provision continues to be appropriate and that the language is sufficiently clear.
I.A.3.8.3	Pending dispute related to a previous transfer, pursuant to the Transfer Dispute Resolution Policy.	Pending dispute related to a previous transfer, pursuant to under the Transfer Dispute Resolution Policy.	This revision is editorial in nature. It is not intended to change the meaning of the provision.
I.A.3.8.4	URS proceeding or URS suspension that the Registrar has been informed of.	Pending URS proceeding or URS suspension that the Registrar has been informed notified of by the Provider in accordance with the URS Procedure.	The term “pending” has been added for consistency with language in I.A.3.8.1 and I.A.3.8.3. In addition, the working group has refined the current text in an effort to clarify that Registrars must deny inter-Registrar transfer requests that are received after a Registrar has been notified by a URS Provider of a URS proceeding or URS suspension in accordance with the URS Procedure.
I.A.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	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	The working group is removing this text entirely as the working group recommends removal of the 60-day inter-Registrar transfer lock from the Change of Registrant Data Policy. (See Rec. 26.4 and associated

	transfer lock prior to the Change of Registrant request.	Change of Registrant request.	rationale for further information).
--	--	--	-------------------------------------

Policy Impact:

LOW - Textual changes for clarity.

Recommendation Rationale:

The working group reviewed the reasons a Registrar MUST deny an inter-Registrar transfer request and proposed textual edits for clarity to both Registrars and registrants.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[h1](#), [h2](#)

Recommendation #24: Revised Reasons that a Registrar of Record MUST NOT Deny a Transfer

The working group recommends changing the following reasons that the Registrar of Record currently MAY NOT deny a transfer into reasons that the Registrar of Record MUST NOT deny a transfer and revising the text as follows:

Reference	Current Text	Revision	Rationale
I.A.3.9.1	Nonpayment for a pending or future registration period.	<u>Implementation Guidance Regarding the Auto-Renew Grace Period</u> : Registrars are prohibited from denying domain name transfer requests based on non-payment of fees for pending or future registration periods during the Auto-Renew Grace Period, provided that any auto-renewal costs borne by the Registrar are reversible for future period.	The working group has provided Implementation Guidance in response to input from ICANN's Contractual Compliance Department that it would be helpful to provide additional guidance consistent with the Registrar Advisory dated 3 April 2008 which states, "Pursuant to the Transfer Policy, registrars are prohibited from denying domain name transfer requests based on non-payment of fees for pending or future registration periods during the Auto-Renew Grace Period."
I.A.3.9.2	No response from the Registered Name Holder or Administrative Contact.	No response from the Registered Name Holder. or Administrative Contact	Under the Registration Data Policy, Administrative Contact data is no longer collected by the registrar. Accordingly, the RNH would be the only authorized transfer contact. This update is consistent with Recommendation 1.
I.A.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.	A Registrar-applied inter-Registrar transfer lock is in place on the Domain name in Registrar Lock Status , for reasons other than those specified in I.A.3.7 and I.A.3.8 unless and the Registered Name Holder is not provided with the reasonable opportunity and ability to unlock the domain name prior to the Transfer Request pursuant to the requirements in sections I.A.5.1 - I.A.5.4.	The updates are primarily intended to improve clarity of the provision, use terminology that will be understood, and refer to the relevant provisions that should be referenced alongside I.A.3.9.3.

I.A.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.	Domain name registration period time constraints, other than as defined in I.A.3.7.5 and I.A.3.7.6 ¹² 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.	The working group updated the language to reference the applicable provisions of the policy rather than repeating the details of those provisions.
I.A.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.	General payment defaults between Registrar and Reseller, as defined in the RAA, business partners / affiliates in cases where the Registered Name Holder for the domain in question has paid for the registration.	The update is not intended to change the meaning of the provision, but rather to update legacy language to be consistent with currently used and defined terminology.

Policy Impact:

LOW - Textual changes for clarity.

Recommendation Rationale:

The working group reviewed the reasons a Registrar MUST DENY an inter-Registrar transfer request and proposed textual edits for clarity.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[h1](#)

¹² In implementation, to the extent that there is renumbering of applicable provisions, this reference should be updated accordingly.

Policy Recommendations and Impact Analysis - Group 1(b)

Introduction to Group 1(b) Recommendations

Change of Registrant (CoR) requirements were recommended by the [IRTP Working Group C](#) to ensure that certain changes to registrant information have been authorized by requiring Registrars to obtain confirmation from the Prior Registrant¹³ and New Registrant¹⁴ before these changes are made. Specifically, CoR policy requirements are applicable under the Transfer Policy when a material change¹⁵ 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. The working group comprehensively reviewed the CoR requirements and is proposing the following changes.

Recommendation #25: Change of Registrant Data

The working group recommends that the Transfer Policy and all related policies MUST use the term “Change of Registrant Data” in place of the currently-used term “Change of Registrant”. This recommendation is for an update to terminology only and does not imply any other changes to the substance of the policies.

25.1: “Change of Registrant Data” is defined as a Material Change to the Registered Name Holder’s name or organization, or any change to the Registered Name Holder’s email address, subject to the language in 25.3.

25.2: The working group affirms that the current definition of “Material Change” remains applicable and fit for purpose.

¹³ 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.

¹⁴ 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.

¹⁵ 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.

25.3: A “Change of Registrant Data” does not apply to the addition or removal of Privacy/Proxy Service Provider (P/P) data in RDDS when such P/P services are provided by the Registrar or its Affiliates.

Policy Impact:

25: **LOW** - Update to terminology only.

25.1: **LOW** - Confirms status quo.

25.2: **LOW** - Confirms status quo.

25.3: **MEDIUM** - Provides new guidance on the addition/removal of privacy/proxy services, i.e., the addition or removal of a P/P service does not constitute a Change of Registrant Data.

Recommendation Rationale:

The working group believes this updated terminology and text related to exceptions more clearly denotes the purpose of the policy, and helps ensure that it is followed where relevant and appropriate. In discussing the addition and removal of Privacy/Proxy data, the working group decided to exclude this from the definition of Change of Registrant Data because these changes were not considered relevant or appropriate for a Change of Registrant Data.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[d2](#), [d3](#), [d9](#), [d10](#), [e2](#), [j1](#)

Recommendation #26: Standalone Policy and Updates to Section II of Transfer Policy

The working group recommends eliminating Section II from the Transfer Policy; instead, the working group recommends that a standalone “Change of Registrant Data” policy **MUST** be established, existing outside of the revised Transfer Policy. For the avoidance of doubt, the working group is not recommending a new PDP to establish this standalone policy; instead, the working group is recommending the Change of Registrant Data Policy be created as part of the implementation of these policy recommendations. As part of the implementation of the new standalone Change of Registrant Data Policy, the working group recommends the following changes from the existing policy language in Section II of the Transfer Policy.

26.1: The working group recommends that the role and definition of “Designated Agent” is no longer fit for purpose. Accordingly, the working group recommends all references to Designated Agent MUST be eliminated from the future standalone Change of Registrant Data Policy.

26.2 The working group recommends eliminating Section II.B “Availability of Change of Registrant” from the future standalone Change of Registrant Data Policy.

26.3 The working group recommends eliminating from the future Change of Registrant Data Policy the requirement that the Registrar request and obtain confirmation from both the Prior Registrant and the New Registrant prior to processing a Change of Registrant Data as detailed in Sections II.C.1.2 and II.C.1.4 of the Transfer Policy.

26.4: The working group recommends eliminating from the future Change of Registrant Data Policy the requirement that the Registrar impose a 60-day inter-Registrar transfer lock following a Change of Registrant. This requirement is detailed in section II.C.2 of the Transfer Policy. Additionally, the working group recommends eliminating from the Transfer Policy the text regarding opting out of the 60-day lock, as this text has been overtaken by the removal of the lock requirement from the Transfer Policy.

Policy Impact:

26: **LOW** - Recommendation suggests separation of policies only.

26.1 MEDIUM - Change from status quo, which will require planning and system changes for Registrars. This recommendation is not meant to explicitly prohibit the use of designated agents or representatives in other contexts where this is allowable.

26.2 LOW - Current requirements under Section II.B are largely duplicative of existing policies and therefore do not need to be restated.

26.3 HIGH - Removal of requirements to obtain confirmation from Prior and New Registrant

26.4 HIGH - Removal of post-Change of Registrant Data transfer restriction (AKA 60-day lock)

Recommendation Rationale:

The working group believes separating the two policies is the best way to ensure that the Change of Registrant Data (CORD) process is clearly documented and defined. The CORD is not a Registrar transfer and, accordingly, the requirements should reside in a standalone policy. Additionally, the working group believes the CORD process should be available at any time during a domain’s registration period. Rationale regarding the working group’s proposed elimination of the 60-day lock can be found in its responses to Charter Questions d4-d8.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[d2](#), [d3](#), [d4](#), [d5](#), [d6](#), [d7](#), [d8](#), [d12](#), [d13](#), [d14](#), [d15](#), [d16](#), [d17](#), [e2](#), [j1](#)**Recommendation #27: Change of Registrant Data Notification**

As part of the implementation of the new standalone Change of Registrant Data Policy, the working group recommends that, following a Change of Registrant Data and ***subject to the opt out requirements described in Recommendation 28***, the Registrar **MUST** send a Change of Registrant Data notification to the Registered Name Holder without undue delay, but no later than 24 hours after the Change of Registrant Data occurred. (emphasis added)

27.1: This notification **MUST** be written in the language of the registration agreement and **MAY** also be provided in English or other languages.

27.2: The Registrar **MUST** include the following elements in the Change of Registrant Data notification:

- Domain name(s)
- Text stating which registrant data field(s) were updated
- Date and time that the Change of Registrant Data was completed
- Instructions detailing how the registrant can take action if the change was invalid (how to initiate a reversal)

27.3: The Registrar **MUST** send the notification via email, SMS, or other secure messaging system. These examples are not intended to be limiting, and it is understood that additional methods of notification may be created that were not originally anticipated by the working group.

27.4: When a change to the Registered Name Holder's email address occurs, and subject to the opt out requirements described in Recommendation 28:

- a. the Registrar **MUST** send the Change of Registrant Data notification to the RNH's prior email address (the email address that was on file with the Registrar immediately prior to the change).

- b. the Registrar MAY send the Change of Registrant Data notification to the RNH's new email address.
- c. the Registrar MAY additionally send the Change of Registrant Data notification to the RNH via SMS or other secure messaging system.

27.5: The Registrar MAY send additional notifications resulting from changes to the Registered Name Holder's phone number, postal address, Account Holder information, or other contact information used by the Registrar to associate the RNH with their domain name or relevant account.

27.6: To the extent that the Change of Registrant Data is requested for multiple domains, and the Registered Name Holder is the same for all domains, the Registrar of Record MAY consolidate the Change of Registrant Data notifications into a single notification.

27.7: To the extent that the Change of Registrant Data may incur a verification request to be sent to the Registered Name Holder pursuant to the RDDS Accuracy Program Specification, the Registrar of Record MAY consolidate the optional Change of Registrant Data notification and the verification request into a single notification, where applicable.

Policy Impact:

HIGH - Read together with Recommendation 28, these two recommendations (Rec. 27 and Rec. 28) have a high impact, in that a mandatory notification is now a notification that registrants may opt out of.

Recommendation Rationale:

The working group believes that notifying the RNH of the CORD update helps to ensure that unintended or unexpected changes are caught and addressed promptly. Further, many RNHs prefer not to receive this type of notification, so the working group recommends they be permitted to opt out of having their registration data used for this purpose (See Recommendation 28). Regarding the language and required elements of the CORD notification, the working group wants to ensure the RNH understands the language of the notification and is empowered with full context of the update.

The working group believes it is important to ensure that the RNH receives this information. The group also recognizes that communications methods change with time and technological advances, and that Registrars may have different preferred paths for communication based on

their relationships with their registrants. The working group understands that the Registrar should be able to determine the best communication method and experience for the RNH.

Regarding the RDDS Accuracy Program Specification (RAPS), the working group recognizes that these two processes are related and may be used together for the best registrant experience.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[d5](#), [d8](#)

Recommendation #28: Opt out of Change of Registrant Data Notification

The working group recommends that the Registrar MAY provide Registered Name Holders with the option to opt out of receiving Change of Registrant Data notifications. IF the Registrar chooses to provide the Change of Registrant Data notification opt-out option to the Registered Name Holder, THEN the following recommendations apply:

28.1: The Registrar MUST enable Change of Registrant Data notifications by default (i) when a domain name is initially registered AND (ii) when a domain name is transferred in from another Registrar.

28.2: If the Registered Name Holder elects to opt out of Change of Registrant Data notifications, the Registrar MAY disable Change of Registrant Data notifications, provided the opt out occurs AFTER initial domain name registration or the completion of an inter-Registrar transfer.

28.3: The Registrar MUST provide clear instructions for how the Registered Name Holder can opt out of (and opt back in to) Change of Registrant Data notifications. Additionally, the Registrar MUST provide warning of the consequences associated with opting out of these notifications, enabling the RNH to make an informed decision whether to opt out.

28.4: The Registrar MUST maintain a record demonstrating that the Registrar validated that the opt-out was requested by the Registered Name Holder. The Registrar MUST retain this record for a period of no fewer than fifteen (15) months following the end of the Registrar's sponsorship of the registration.

28.5: The Change of Registrant Data notification opt-out option does not apply to any verification notices sent pursuant to the RDDS Accuracy Program Specification.

28.6: The Registrar MAY modify their opt-out option at the data field level. For example, a Registrar may choose to offer an opt out for material changes to the Registrant Name or Registrant Organization but not allow an opt out for a change to the Registered Name Holder's email address.

Policy Impact:

HIGH - Read together with Recommendation 27, these two recommendations (Rec. 27 and Rec. 28) have a high impact, in that a mandatory notification is now a notification that registrants may opt out of.

Recommendation Rationale:

The working group believes it is beneficial to ensure that the RNH is notified of changes to their domain registration data, in case the change was inadvertent (e.g., they thought they were updating a different domain) or unauthorized (e.g., someone accessed their account without permission), while the RNH should also be empowered to turn off these notices.

The working group understands that these notifications are a personal data processing activity which may not be deemed absolutely necessary, and so the working group recommends the RNH be able to decide if they want to receive these notices or not. Since the notification is sent for security purposes, it should be required by default with the option to turn it off provided. The working group also believes the mandatory provision of the consequences associated with opting out of these notifications will help the RNH understand their options which have security benefits.

Regarding the RDDS Accuracy Program Specification (RAPS), the working group believes RAPS is for a different purpose and should not be affected by this CORD process.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[d8](#)

Policy Recommendations and Impact Analysis - Group 2

Introduction to Group 2 Recommendations

Transfer Emergency Action Contact (TEAC)

According to Section I. A.4.6 of the Transfer Policy, Registrars are required to designate a Transfer Emergency Action Contact (TEAC) to facilitate urgent communications relating to inter-Registrar transfers with the goal of quickly establishing a real-time conversation between Registrars in case of an emergency.

Transfer Dispute Resolution Policy (TDRP)

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.

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.

During discussions on the Group 2 topics, the working group reviewed the TEAC, TDRP, and ICANN-approved transfers and is proposing the following changes.

Recommendation #29: Timing for Responding to Contact from a Transfer Emergency Action Contact (TEAC)

Section I.A.4.6.3 of the Transfer Policy states, "Messages sent via the TEAC communication channel must generate a non-automated response by a human representative of the Gaining Registrar. The person or team responding must be capable and authorized to investigate and address urgent transfer issues. Responses are required within 4 hours of the initial request, although final resolution of the incident may take longer." The working group recommends that the policy must be revised to update the required timeframe for initial response from 4 hours to 24 hours / 1 calendar day.

Policy Impact:

LOW - Time for responding to communications via the TEAC communication channel has been extended from 4 hours to 24 hours, reducing the operational burden on Registrars while still requiring timely response.

Recommendation Rationale:

The working group agreed that a longer timeframe for initial response to a TEAC request is warranted due to concerns around the tight 4-hour timeframe and the significant consequences associated with missing the deadline. The working group noted that the RAA provides a 24-hour deadline for Registrars to provide an initial, non-automated response to reports of illegal activity, although final resolution of the underlying issue may take longer. The working group observed that communication to a TEAC could be considered an analogous use case and agreed that a 24-hour time frame for initial response is acceptable for handling emergencies, while addressing concerns raised by Registrars about the operational impacts of TEAC requirements and associated risks of misuse.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[f2](#), [f3](#)

Recommendation #30: Timing for Additional Interactions with the TEAC

Section I.A.4.6.2 of the Transfer Policy states in part, “. . . 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 working group recommends that the Transfer Policy must be updated to state that the initial communication to a TEAC is expected to occur no more than 30 days following the alleged unauthorized loss of a domain. If the initial communication to the TEAC occurs more that 30 days following the alleged unauthorized loss of a domain, the Losing Registrar must provide a detailed written explanation to the Gaining Registrar’s TEAC justifying why this is an emergency situation that must be addressed through the TEAC communication channel and providing information about why earlier contact to the TEAC was not possible.

Policy Impact:

LOW - Sets a new outer bound for communications to a TEAC. The majority of initial communications to the TEAC already occur within this outer bound, making this a low impact change.

Recommendation Rationale:

The text of this recommendation sets clear and consistent expectations regarding a “reasonable period of time” while allowing flexibility to use the TEAC communication channel outside of this timeframe under exceptional circumstances that may still constitute an emergency. Under such circumstances, the Gaining Registrar must provide the Losing Registrar with a written justification. As discussed in the working group’s response to charter question f4, the 30-day timeframe for initial contact aligns with the 30-day transfer restriction following initial registration and inter-Registrar transfer, detailed in recommendations 16 and 17.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[f4](#)

Recommendation #31: Additional Communications with TEAC

Once a Gaining Registrar has provided an initial non-automated response to a TEAC communication as described in Section I.A.4.6.3 of the Transfer Policy, the Gaining Registrar must provide additional, substantive updates by email to the Losing Registrar at least every 72 hours / 3 calendar days until work to resolve the issue is complete. These updates must include specific actions taken by the Gaining Registrar to work towards resolution.

Policy Impact:

MEDIUM - New requirement for response time for Registrars, which will require planning and system changes.

Recommendation Rationale:

The working group agreed that it is important for a Gaining Registrar to demonstrate progress towards resolving an issue raised through the TEAC communication channel. The working group further agreed the policy needs to provide some degree of flexibility with respect to timeframe

for resolution, given that each case is unique. A requirement to provide regular updates introduces transparency and accountability, without setting strict deadlines that may not be appropriate or feasible to meet, even when both Registrars are working diligently towards resolution of the issue. In determining the frequency of updates, the working group agreed that it is appropriate to require updates every 72 hours / 3 calendar days. Updates at this cadence provide clear indication to the Losing Registrar as to whether resolution is proceeding while not being excessively burdensome to the Gaining Registrar who is required to provide the updates.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[f4](#)**Recommendation #32: Method of Communication with TEAC**

The working group recommends that initial communication to the TEAC described in Section I.A.4.6.2 of the Transfer Policy must either be in the form of email or, if the primary TEAC communication channel is designated as a phone number or other method, the verbal/non-email communication MUST be accompanied by an email communication to the TEAC. This email “starts the clock” for the response timeframe specified in Recommendation 29.

Policy Impact:

MEDIUM - Policy change to initial communication with TEAC, which may involve planning and system changes for Registrars.

Recommendation Rationale:

As described in the WG’s response to Charter Question f5, requiring the initial TEAC exchange by email ensures that there is a paper trail associated with each initial TEAC contact without creating complex new requirements for a system of record that may be seldom used.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[f5](#)

Recommendation #33: Request to GNSO for further work on Transfer Dispute Resolution Policy and Potential New Dispute Mechanism

The working group recommends the GNSO request an Issues Report or other suitable mechanism to further research and explore the pros and cons of (i) expanding the TDRP to registrant filers and (ii) creating a new standalone dispute resolution mechanism for registrants who wish to challenge improper transfers, including compromised and stolen domain names. In making this recommendation, the working group recognizes that if such an effort were ultimately adopted by the GNSO Council, this request could be resource-intensive and will require the Council to consider the appropriate timing and priority against other policy efforts.

Policy Impact:

LOW/HIGH - The changes, or lack of changes, to the TDRP results in a low impact to the policy; however, the high indication denotes the potential future policy work in completing an Initial Report on the requested issues.

Recommendation Rationale:

Because the working group observed that many issues fall outside the limited scope of the TDRP, it believes further policy work is needed in terms of potential expansion of the TDRP and/or creating a new dispute mechanism. By way of example, many registrant concerns and issues with unauthorized inter-Registrar transfers fall outside the limited scope the TDRP is designed to address. For example, a bad actor may compromise a registrant's account, update contact details, retrieve the AuthInfo Code, and transfer a domain name to another Registrar without the authorization of the registrant. This type of transfer may technically comply with the Transfer Policy, provided the required steps are followed, even though the domain name was compromised prior to the transfer.

Additionally, the working group discussed the pitfalls and disadvantages provided by the IRTF WG Part D with respect to registrant access to the TDRP. The working group noted that if a registrant believes an improper transfer has taken place, and its previous Registrar of record is either unresponsive or unable to resolve the issue informally and/or the previous Registrar is unwilling to file a TDRP complaint, the registrant is left with unfavorable options. The registrant could choose to file a complaint with ICANN compliance; however, ICANN compliance does not have the authority to reverse a transfer. The registrant could also choose to go to court; however, that option can be prohibitively expensive, especially compared to the cost of filing a TDRP complaint.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[g3](#)**Recommendation #34: Fees Associated with Voluntary Full Portfolio Transfers over 50,000 domain names**

34.1: The working group recommends that a Registry Operator MAY charge a fee to implement a full domain name portfolio transfer¹⁶ of 50,000 or more domain names from one ICANN-accredited Registrar to another ICANN-accredited Registrar(s)¹⁷, provided the conditions described in sections I.B.1.1 and I.B.1.2 are satisfied.

34.2: The Registry MAY waive the fee associated with full portfolio transfers; however, in full portfolio transfers resulting from an involuntary Registrar termination, i.e., where a Registrar is terminated by ICANN due to non-compliance with the Registrar Accreditation Agreement, the working group recommends the Registry MUST waive any fee associated with a full portfolio transfer.

Policy Impact:

LOW -Retention of status quo. (34.1)

LOW - Involuntary full portfolio transfers, resulting from Registrar or RRA terminations AND involving greater than 50,000 names are very rare, and, accordingly, this recommendation has a low impact. (34.2)

Recommendation Rationale:

The working group deliberated the required fee in I.B.2 at length, and Registry Representatives noted that the fee is in recognition of the administration and coordination required to

¹⁶ Note: this could include all of the domain names a Registrar has within a gTLD or all of the gTLD domain names a Registrar has under management

¹⁷ In the majority of instances, ICANN org will choose one Gaining Registrar to take over the Losing Registrar's domain name portfolio; this is the preferred scenario to avoid customer confusion. However, there may be a situation where multiple Gaining Registrars will be chosen. For example, if there is no Registrar who offers all of the TLDs of the Losing Registrar, ICANN org will need to identify more than one Gaining Registrar to which the domain names will be transferred to.

implement a full portfolio transfer. Accordingly, the working group agreed that in the case of a voluntary full portfolio transfer, the Registry may charge a fee, but the Registry may not charge a fee in the event of an involuntary full portfolio transfer. The working group noted the challenges in securing a Gaining Registrar for involuntary full portfolio transfers, as described by ICANN org, and agreed the fee should be waived in these limited instances.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i1](#)

Recommendation #35: Retainment of Current Full Portfolio Transfer Fee Ceiling and Minimum Domain Name Threshold

The working group recommends retaining both (i) the current minimum number of domain names that trigger the fee at 50,000 names and (ii) the current price ceiling of USD \$50,000. If the full portfolio transfer involves multiple Registry Operators, the affected Registry Operators MUST ensure the collective fee does not exceed the recommended ceiling of USD \$50,000, and the fee MUST be apportioned based on the number of domain names transferred.

Policy Impact:

HIGH - The recommendation, in combination with Recommendations 36-38 introduces the idea of a collective fee and various requirements associated with this new calculus. Specifically, rather than a threshold of 50,000 domain names PER TLD, this involves a threshold of 50,000 domain names across all TLDs, which significantly increases the amount of full portfolio transfers where fees are involved. Additionally, these recommendations create new coordination requirements for Registrars, Registries, and ICANN org.

Recommendation Rationale:

The working group has noted retaining a price ceiling promotes transparency and has recommended keeping the status quo; however, the working group believes it is important to specify the price ceiling encompasses a collective fee. In other words, the USD \$50,000 fee is the total amount a registrar would pay for a voluntary full portfolio transfer. The working group made this update in recognition of the changes to the industry that have occurred since this policy was first drafted, i.e., the number of Registry Operators and TLDs has increased significantly, which could result in unintended high fees.

Implementation Guidance:

The recommendation notes that the fee must be apportioned based on the number of domain names transferred. In practice, this means that if there are 60,000 total domain names transferred and 30,000 domain names are .example names, and 30,000 domain names are .illustration names, the .example registry could charge up to USD \$25,000 and the .illustration registry could charge up to USD \$25,000. This is because the two Registries each transferred 50% of the domain names; accordingly, each registry may charge 50% of USD \$50,000, which is the price ceiling referenced in Recommendation 35.

Links to Charter Question(s) & Summary of Deliberations:

[i1](#)

Recommendation #36: Restriction of Fee Adjustments for Full Portfolio Transfers Involving Multiple Registry Operators

The working group recommends that if the full portfolio transfer involves multiple Registry Operators, and one or more affected Registry Operators chooses to waive its portion of the collective fee, the remaining Registry Operators MUST NOT adjust their fees to a higher percentage due to another Registry Operator's waiver.

Policy Impact:

HIGH - The recommendation, in combination with Recommendations 35, 37-38, introduces the idea of a collective fee and various requirements associated with this new calculus. Specifically, rather than a threshold of 50,000 domain names PER TLD, this involves a threshold of 50,000 domain names across all TLDs, which significantly increases the amount of full portfolio transfers where fees are involved. Additionally, these recommendations create new coordination requirements for Registrars, Registries, and ICANN org.

Recommendation Rationale:

The working group notes the fee apportionment was designed to be equitable, and this recommendation aims to ensure a voluntary fee waiver does not result in an unintended consequence or gaming.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[i1](#)**Recommendation #37: Registry Operator Notice to ICANN of Full Portfolio Transfer Completion**

The working group recommends that following the completion of the transfer, the Registry Operator(s) MUST provide notice to ICANN that the transfer is complete, and the notice to ICANN MUST include the number of domain names transferred.

Policy Impact:

HIGH - The recommendation, in combination with Recommendations 35-36, 38, introduces the idea of a collective fee and various requirements associated with this new calculus. Specifically, rather than a threshold of 50,000 domain names PER TLD, this involves a threshold of 50,000 domain names across all TLDs, which significantly increases the amount of full portfolio transfers where fees are involved. Additionally, these recommendations create new coordination requirements for Registrars, Registries, and ICANN org.

Recommendation Rationale:

As the entity responsible for effecting the transfer, the Registry Operator is responsible for providing the official number of domain names transferred to ICANN.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[i1](#)

Recommendation #38: ICANN Notice to Affected Registry Operators of Associated Domain Name Numbers for Full Portfolio Transfers

The working group recommends that following receipt of notices from all affected Registry Operators, ICANN MUST send a notice to affected Registry Operators with the reported numbers and corresponding percentages of domain names involved in the bulk transfer, e.g., 26% of names for .ABC and 74% of names for .DEF. The Registry Operators MAY then charge the Gaining Registrar a fee pursuant to the requirements in Recommendation #35 and associated Implementation Guidance.

Policy Impact:

HIGH - The recommendation, in combination with Recommendations 35-37, introduces the idea of a collective fee and various requirements associated with this new calculus. Specifically, rather than a threshold of 50,000 PER TLD, this involves a threshold of 50,000 across all TLDs, which significantly increases the amount of full portfolio transfers where fees are involved. Additionally, these recommendations create new coordination requirements for Registrars, Registries, and ICANN org.

Recommendation Rationale:

The working group noted that ICANN org is the appropriate entity to notify affected Registry Operators of the numbers transferred after receiving notice from the affected Registries. The working group provided example percentages for clarity of implementation.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i1](#)

Recommendation #39: Gaining Registrar Responsibility for Payment of Fees Associated with Full Portfolio Transfer

The working group recommends that the Gaining Registrar MUST be responsible for paying any relevant Registry fees related to any voluntary full portfolio transfer that it initiated and approved.

Policy Impact:

LOW - Maintains but clarifies the status quo.

Recommendation Rationale:

The working group recognizes that a voluntary request to transition a domain name portfolio to another registrar will require internal coordination and work from the relevant Registry Operator, and accordingly, the Registry Operator may charge a fee for this process. Due to the voluntary nature of the portfolio transfer request, the Gaining Registrar should be responsible for paying this fee to the Registry Operator as (i) the Gaining Registrar, through the transfer, is inheriting new customers, and (ii) the Losing Registrar may be going out of business and, accordingly, may be unable to pay the fee.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i1](#)

Recommendation #40: Inclusion of Bulk Transfer After Partial Portfolio Acquisition (BTAPPA) in Transfer Policy

The working group recommends updating the Transfer Policy to include the Bulk Transfer After Partial Portfolio Acquisition (BTAPPA) directly into the Transfer Policy, which would apply to all Registry Operators.¹⁸

Policy Impact:

HIGH - This recommendation involves a significant expansion of the BTAPPA service.

Recommendation Rationale:

The working group believed this creates more consistency across all Registries.

¹⁸ For the avoidance of doubt, the working group is recommending that the BTAPPA would be included as part of the Transfer Policy, and when the updated Transfer Policy becomes effective, Registry Operators will no longer have to file an RSEP to offer the BTAPPA.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[i2](#)

Recommendation #41: Expansion of BTAPPA to Registrar Agents

The working group recommends that the standard Bulk Transfer After Partial Portfolio Acquisition (BTAPPA) be expanded to include circumstances where an agent of the Registrar, such as a Reseller or service provider, elects to transfer its portfolio of domain names to a new gaining registrar, and the registration agreement explicitly permits the transfer.

Policy Impact:

HIGH - This recommendation involves a significant expansion of the BTAPPA service.

Recommendation Rationale:

The working group supported an expansion of the BTAPPA to allow for additional partial bulk transfers, such as Resellers or service providers to transfer their names to a different sponsoring registrar. The working group recognized there are situations where this may be necessary, such as when Registrar's agent (such a reseller) may need to change its sponsoring registrar due to data privacy concerns within a particular jurisdiction, and there is currently not a way to do this that does not involve a significant manual effort.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:[i2](#)

Recommendation #42: Required Registrar Notification of BTAPPA

In the event of a BTAPPA, the Registrar shall either notify or ensure its Resellers (where applicable) notify affected Registrants approximately one month¹⁹ / at least 30 calendar days before the change of sponsorship is expected to occur. This notification²⁰ must provide instructions on (i) how to opt out (if applicable), (ii) how to transfer the name to a registrar other than the Gaining Registrar before the date of the sponsorship change, if desired, (iii) the expected date of the change of sponsorship, (iv) the name of the Gaining Registrar, and (v) a link to the Gaining Registrar's (or their Reseller's) terms of service.

Policy Impact:

MEDIUM - New notice requirement for Registrars.

Recommendation Rationale:

Advance notice will give affected registrants the ability to transfer their name elsewhere if they so desire or opt out of the transfer if that option is available. In some instances, such as a registrar consolidation where a registrar will cease to exist upon the transfer, the option to opt out may not be available. Clarifying when the transfer will take place, to which registrar it will transfer, and what their terms of service are enables registrants to familiarize themselves with the new registrar and their terms before the change of sponsorship takes place.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i2](#)

¹⁹ The WG recognizes that some flexibility is required in the timing of Change of Sponsorship (BTAPPA) notifications. As such, one month should be treated as no less than 26 and no more than 35 days. A Registrar is not precluded from sending additional notifications earlier or later than this required one month notification.

²⁰ A notice MAY encompass multiple TLDs if a Registered Name Holder has registered domain names under more than one TLD and the same parameters apply to the transfers, i.e., the date of transfer, instructions, etc.

Recommendation #43: Domain Name Expiration Dates During BTAPPA

The working group recommends that for a change of sponsorship, the expiration dates of transferred registrations are not affected, and, therefore, there are no ICANN fees. Once the change of sponsorship is complete, the working group recommends that there is no grace period to reverse a transfer.

Policy Impact:

LOW - Status quo (current boilerplate language in BTAPPA).

Recommendation Rationale:

The working group reviewed the language in the BTAPPA boilerplate and noted this is an important provision to include in the Transfer Policy. Because this is a transfer initiated by the registrar rather than the registrant, there is no change to the expiration date.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i2](#)

Recommendation #44: Permitted Rejection of BTAPPA Request

The working group recommends a Registry Operator **MUST** reject a change of sponsorship request if there is reasonable evidence that the change of sponsorship is being requested in order to avoid fees otherwise due to the Registry Operator or ICANN. A Registry Operator has discretion to reject a change of sponsorship request if a registrar with common ownership or management or both has already requested a change of sponsorship within the preceding six-month period.

Policy Impact:

LOW - Status quo (current boilerplate language in BTAPPA).

Recommendation Rationale:

The working group reviewed the language in the BTAPPA boilerplate and noted this is an important provision to include in the Transfer Policy because it allows discretion for Registry Operators to reject BTAPPA requests under certain circumstances.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i2](#)

Recommendation #45: Required Registration Agreement Language for BTAPPA

The working group recommends the Losing Registrar's existing Registration Agreement with customers MUST permit the transfer of domain names in the event of the scenarios described in the Transfer Policy with respect to a change of sponsorship. Additionally, the Losing Registrar's Registration Agreement MUST inform registrants that in the event of a change of sponsorship, the affected registrants will be deemed to have accepted the new registrar's terms, unless the registrant transfers their domain name(s) to a different registrar prior to the change of sponsorship.

Policy Impact:

LOW - This may require changes to some registrars' registration agreement to allow for these transfers.

Recommendation Rationale:

The working group added this language to ensure registrants receive notice via their registration agreements.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i2](#)

Recommendation #46: Notice of Registry Fees for BTAPPA

The working group recommends that a Registry Operator MAY charge a fee for a change of sponsorship, but Registry Operators MUST provide notice to Registrars of any fees associated with a change of sponsorship upon request and prior to the initiation of the transfer. How Registry Operators choose to provide notice of fees will be up to the Registry to decide, i.e., password protected portal, website, written notice, etc.

Policy Impact:

MEDIUM - May involve changes for Registries, which could include planning and system changes.

Recommendation Rationale:

The policy language clarifies that Registries may charge a fee; however, in order to do so, they must provide notice to registrars.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i2](#)

Recommendation #47: Prohibition on Post-BTAPPA Transfer Restriction

The working group recommends that in the case of a change of sponsorship, the Gaining Registrar MUST NOT impose a new inter-registrar transfer lock preventing affected registrants from transferring their domains to another Registrar.

Policy Impact:

MEDIUM - New requirements may trigger planning and system changes for registrars.

Recommendation Rationale:

The working group notes that a change of sponsorship is not initiated by registrants and does not affect their domain name expiration dates; therefore, the transfer lock that would

otherwise follow a typical inter-registrar transfer should not apply in this instance. Transfer locks that are triggered by other means set out in the Transfer Policy would still apply.

Implementation Guidance:

N/A

Links to Charter Question(s) & Summary of Deliberations:

[i2](#)

Annex 1 – Original Working Draft Recommendation Order

As noted in the introduction, the working group initially used a recommendation order based on the order of the charter questions. To reduce size and complexity in the core of the Final Report, the recommendations were re-ordered to allow for easier readability and comprehension. The list below acts as a reference to the older numbering system. Only Group 1A recommendation numbers were affected. The remaining recommendations numbers for Groups 1B & 2 are not listed here.

- Rec 1 (~~6~~): Terminology Updates: Whois
- Rec 2 (~~17~~): Terminology Updates: Administrative Contact and Transfer Contact
- Rec 3 (~~18~~): Transfer Restriction After Initial Registration
- Rec 4 (~~7~~): Update Term “AuthInfo Code” to “Transfer Authorization Code (TAC)”
- Rec 5 (~~8~~): TAC Definition
- Rec 6 (~~14~~): Service Level Agreement (SLA) for TAC Provision
- Rec 7 (~~9~~): TAC Composition
- Rec 8 (~~10~~): Verification of TAC Composition
- Rec 9 (~~15~~): TAC Time to Live (TTL)
- Rec 10 (~~11~~): TAC Generation, Storage, and Provision
- Rec 11 (~~4~~): Notification of TAC Issuance
- Rec 12: Verification of TAC Validity
- Rec 13 TAC is One-Time Use
- Rec 14 (~~2~~): Maintenance of Records
- Rec 15 (~~1~~): Gaining FOA
- Rec 16 (~~6~~): Registry Transmission of IANA ID to Losing Registrar
- Rec 17 (~~3~~): Losing FOA
- Rec 18 (~~19~~): Transfer Restriction After Inter-Registrar Transfer
- Rec 19 (~~5~~): Notification of Transfer Completion
- Rec 20: Format of Transfer Policy Section I.A.3.7
- Rec 21: Revised Reasons that a Registrar of Record MAY Deny a Transfer
- Rec 22: New Reasons that a Registrar of Record MUST Deny a Transfer
- Rec 23: Revised Reasons that a Registrar of Record MUST Deny a Transfer
- Rec 24: Revised Reasons that a Registrar of Record MUST NOT Deny a Transfer
- Rec 25: Change of Registrant Data
- Rec 26: Standalone Policy and Updates to Section II of Transfer Policy
- Rec 27: Change of Registrant Data Notification
- Rec 28: Opt out of Change of Registrant Notification

Return to [Group 1A Introduction](#)

Annex 2 – Group 1(a) Charter Questions and WG Summary Deliberations

[Link](#) to TPR WG Charter.

Gaining Registrar FOA and Losing Registrar FOA

Charter Question: Gaining FOA and Losing FOA

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

Summary of Deliberations:

The Inter-Registrar Transfer Policy - Part D Policy Development Process Working Group (IRTP WG D), previously examined the question of “Whether the universal adoption and implementation of Extensible Provisioning Protocol (EPP) AuthInfo codes has eliminated the need of FOAs.” The IRTP WG D ultimately determined to retain the FOA until more evidence was gathered. The Transfer Policy Review Working Group was asked to revisit the same question and has determined there is now strong evidence that the Gaining FOA can be eliminated from the Transfer Policy without negatively affecting the security of inter-Registrar transfers. The working group further believes that requirements for a Gaining FOA or a similar replacement are unjustified under data protection law and no longer necessary from a practical perspective to facilitate the transfer. The working group recognizes that this is a significant departure from existing policy and has therefore provided a detailed rationale for its conclusion.

Prior to the General Data Protection Regulation (GDPR) coming into force, the Gaining Registrar was required to confirm the Registered Name Holder’s (RNH) intent to transfer by sending an email to the RNH asking for confirmation to proceed. In order for the Gaining Registrar to be able to send the Gaining FOA, it needed to obtain the RNH’s contact information from the publicly available Registration Data Directory Services (RDDS). With the introduction of the GDPR, Gaining Registrars were no longer able to obtain this information via RDDS, as personally identifiable information was largely redacted within RDDS. In recognition of this new obstacle, ICANN org, after Board approval, deferred Contractual Compliance enforcement on Gaining FOA requirements. While still a requirement on paper, in practice the Gaining FOA does not currently exist and cannot exist.

The working group considered that it could recommend some form of replacement for the Gaining FOA to be included in future policy requirements. If it did so, there would need to be a method and a justification for the Registrar of Record to transfer the RNH's contact information to the Gaining Registrar.

The working group considered that it is likely possible from a technical perspective to facilitate the transfer of the RNH's contact information from the Registrar of Record to the Gaining Registrar for the purposes of confirming the RNH's intent to transfer. However, the working group did not pursue specific methods for doing so because it did not believe this transfer is feasible from a legal perspective.

In its deliberations on applicable law, the working group considered the principles of data minimization and privacy by design. Under these principles, in order to justify the transfer of personally identifiable information (PII) from the Registrar of Record to the Gaining Registrar and the subsequent processing of this data (in order to send the Gaining FOA) by the Gaining Registrar, one would have to demonstrate that this transfer and processing of PII is necessary to facilitate the transfer. The working group noted that the transfer process has functioned without the Gaining FOA since the GDPR went into force, and the working group has not encountered any evidence that there has been an increase in unauthorized transfers since the Gaining FOA was functionally eliminated. It has not found any other indications that the transfer process is malfunctioning without the Gaining FOA requirement. Therefore, the working group sees no evidence that the Gaining FOA is needed for the purpose of facilitating the transfer or protecting the RNH from unauthorized transfers.

The working group notes that the recommendations in this report should be viewed as a package. The recommendations include adjustments and enhancements that seek to provide an appropriate level of security for the inter-Registrar transfer process while also taking into account the customer experience, applicable law, and operational considerations for Registries and Registrars.

The working group looked at the value that the Gaining FOA provided to ensure that equivalent value is covered by newly added elements of the process going forward, as appropriate.

The working group noted that when the Gaining FOA requirements were in place, the transfer could only proceed once the RNH had responded to the Gaining FOA. This meant that the RNH always actively confirmed the intent to transfer before the transfer took place. The Gaining FOA therefore served a notification function and also a confirmation function. To the extent that the party obtaining the Transfer Authorization Code (TAC) and requesting the transfer was an

individual other than the RNH, the RNH had the opportunity to confirm that they were aware of the request and wanted it to proceed.

The working group notes that in the current transfer process, 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. If after five calendar days, the Registry Operator has not received any objection to the inter-Registrar transfer, it will process the transfer request. As detailed in Recommendation 17, the working group anticipates that this element of the transfer process will remain in place, although the working group recommends using the term "Transfer Confirmation" in place of Losing FOA. While the Transfer Confirmation does not require affirmative consent, the working group believes that it does provide an important notification function and also gives the RNH an opportunity to take action prior to completion of the transfer if the transfer is unwanted.

In addition, the working group believes that the new notifications detailed in Recommendations 11 and 17 ensure that the RNH receives the necessary information with respect to an inter-Registrar transfer. These notifications provide instructions on what to do if the RNH wants to either stop or reverse the process because the action on the account is unauthorized or unintended.

The working group noted that while it was in use, the Gaining FOA provided a record to assist ICANN's Contractual Compliance department in investigating complaints, especially those related to unauthorized transfers. It also supported the resolution of disputes. The working group noted that records associated with provision of the TAC, the Transfer Confirmation, and new notifications detailed in Recommendations 11 and 17, will provide the necessary paper trail for this purpose. Recommendation 14 provides specific guidance of record keeping.

The working group recalled that the Gaining FOA pre-dated the Transfer Authorization Code (TAC), formerly referred to as the AuthInfo Code, and that prior to the introduction of the TAC, the Gaining FOA was an essential element for facilitating the transfer and also provided a function that was important to prevent the unauthorized transfer of domains. With the introduction of the TAC, an additional layer of security was added to the process, and the Gaining FOA became less essential. The recommendations in this report further evolve the security model for the transfer process, including with respect to the TAC. The working group believes that the security model presented in the package of recommendations offers the appropriate elements to reduce the risk of unauthorized transfer to the extent possible within the bounds of the Transfer Policy. Key elements of the model include the following:

- The issuance of the TAC is the means of confirming that the RNH intends to transfer the domain. The first and most important line of defense and the primary point of control is logging into the account at the Registrar. This is the “affirmative consent” to initiate the transfer. The working group understands that certain threat vectors, including hacking of the RNH’s email or unauthorized access to the RNH’s account at the Registrar, are legitimate concerns. At the same time, the working group considers them outside the scope of the Transfer Policy and therefore outside the scope of this working group.
- Acknowledging the role that the TAC plays as a token to enable the transfer process, the working group has recommended specific enhancements related to TAC security:
 - Minimum requirements for composition to the TAC (Recommendation 7), seek to reduce the risk of an unauthorized party guessing the TAC to initiate an unauthorized transfer.
 - Limiting when, where, and for how long the TAC may be vulnerable to theft once generated. The TAC is only generated at the point that it is needed to initiate an inter-Registrar transfer (Recommendation 9.1). It is stored securely at the Registry (Recommendation 9.2). The TAC has a maximum lifetime of 14 days, preventing the existence of a long-lived TAC, which could be used as part of an unauthorized or unintended inter-registrar transfer (Recommendation 13).
- Once a domain is transferred, the Registrar must restrict the RNH from transferring a domain name to a new Registrar within 30 days. To the extent that the transfer is unauthorized, this restriction will consistently prevent the transfer of a domain multiple times in rapid succession, a practice associated with domain theft that makes it difficult to recover the domain.

Recommendations: [#15](#)

Charter Question: Gaining FOA and Losing FOA

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

Summary of Deliberations:

As described in the above response to charter question a1, the working group has determined that the Gaining FOA should no longer be a requirement.

Recommendations: N/A**Charter Question: Gaining FOA and Losing FOA**

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?

Summary of Deliberations:

As noted in the response to charter question a1, the working group considered that it is likely possible from a technical perspective to facilitate the transfer of the RNH’s contact information from the Registrar of Record to the Gaining Registrar for the purposes of confirming the RNH’s intent to transfer. However, the working group did not pursue specific methods for doing so because it did not believe this data transfer is feasible from a legal perspective.

Recommendations: N/A**Charter Question: Gaining FOA and Losing FOA**

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

Summary of Deliberations:

As described in the response to charter question a1, the working group believes that the package of recommendations presented in this report provides for a transfer process with appropriate levels of security within the bounds of the Transfer Policy, including enhancements to the security of the Transfer Authorization Code. Please see the response to charter question a1 for additional details.

Recommendations: [#7](#), [#8](#), [#10](#), [#11](#)

Charter Question: Gaining FOA and Losing FOA

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

Summary of Deliberations:

The working group acknowledges that with the elimination of the Gaining FOA requirement, the AuthInfo code becomes even more important for the transaction and for any Compliance investigation related to it. The working group further agrees that it is important to properly document and retain all notifications related to the transfer sent by the Losing Registrar, so that information about such records can be sent to ICANN Compliance when investigating a complaint, as needed. Therefore, the working group is providing a specific recommendation on requirements regarding the retention of these records and provision to ICANN upon reasonable notice.

Recommendations: [#14](#)

Additional Security Measures

Charter Question: 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 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?

Summary of Deliberations:

The working group understands that this charter question refers to a lock that some Registrars apply by default to protect their customers from accidental or malicious inter-Registrar transfers. Registrants may, however, request lock removal, and Registrars must remove the lock within five days per requirements of the Transfer Policy. Charter question a6 asks whether this lock, which some Registrars choose to apply today, should become a policy requirement for ALL Registrars. For the avoidance of doubt, the lock addressed in this charter question is distinct from potential requirements for a Registrar to restrict the RNH from transferring a domain name to a new Registrar within 30 days of the initial registration date and within 30 days of the completion of an inter-Registrar transfer. Unlike Recommendations 3 and 18 regarding inter-Registrar transfer restrictions, the lock discussed in this charter question is a default lock that is generally removable upon the request of the registrant, while the restrictions discussed in Recommendations 3 and 18 are triggered by a specific event and are not removable upon the request of the registrant.

The working group does not believe that mandatory domain name locking as presented above should be added to the Transfer Policy. The working group believes that the security model presented in response to charter question a1 provides for a transfer process with appropriate levels of security within the bounds of the Transfer Policy. It is the working group's view that Registrars are in the best position to determine whether locking a domain by default upon registration is appropriate for their customers in combination with other security features implemented by the Registrar. The working group expects that Registrars will continue to use their own discretion to implement any additional measures that may be appropriate for their business model and customer base.

Recommendations: [#18](#)

Losing FOA

Charter Question: Losing FOA

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

Summary of Deliberations:

The working group extensively discussed the function and utility of the Losing FOA, which the working group recommends re-naming the Transfer Confirmation, both in initial deliberations leading up to publication of the Initial Report and in the context of reviewing public comments on the Initial Report. Ultimately, the working group did not reach agreement to eliminate or substantially change the Obligations of the Registrar of Record described in Section I.A.3.1 - I.A.3.6 of the Transfer Policy, and therefore anticipates that these requirements will largely remain in place with the minor modifications presented in Recommendation 2.

Early working group deliberations revealed that a number of working group members supported eliminating the Transfer Confirmation in light of other working group recommendations that sought to increase security and improve efficiency of the transfer process. Those advocating for this approach raised the following points:

- The working group is recommending that the Registrar of Record must send a Notification of TAC Issuance to the RNH when the TAC is issued and a Notification of Transfer Completion to the RNH following completion of the transfer. These notifications largely fulfill the notification function that is currently provided by the Transfer Confirmation.
- It is not necessary to give the RNH an opportunity to confirm or deny the transfer via the Transfer Confirmation, because the act of logging into the control panel at the Registrar of Record in order to request the TAC is, in itself, an indication of consent. If the registrant has a high-value domain, the registrant should select a Registrar of Record that offers extra features and services to protect the security of the account and domain transactions. It is outside of the scope of the Transfer Policy to address Registrar account security.
- The registrant always has the opportunity to select a Registrar of Record who conducts additional due diligence after the TAC is requested and before the Registrar of Record issues the TAC. The working group has recommended that, as is the case in the current Transfer Policy, the Registrar of Record must have up to 5 days to issue the TAC. If notifications replace the Transfer Confirmation, and the RNH selects a Registrar who takes extra time for due diligence, the RNH will also have additional time to receive and

respond to Notification of TAC Issuance, allowing them to stop the transfer process if it is unwanted.

- The current Transfer Confirmation process can delay the transfer for up to an additional five calendar days. By eliminating the Transfer Confirmation, the working group reduces the overall maximum time of the transfer process, making it possible to transfer a domain almost instantaneously, which is beneficial for some registrants.
- The working group is recommending additional security features, which will reduce the security risks associated with transfers. In particular, the working group has recommended that the TAC must be generated on demand, reducing the window of time in which the TAC is vulnerable to theft. In addition, the recommended 30-day post-transfer lock helps to ensure that if a domain is stolen, domain hopping will be slowed, allowing the Losing and Gaining Registrars to work together to resolve the problem.
- In the current process, the Transfer Confirmation has limited utility in a common attack scenario. Specifically, if an attacker obtains access to the control panel, the attacker can change the recipient of the Transfer Confirmation to the attacker's own email address, thereby eliminating the utility of the Transfer Confirmation.

In line with the above points, the working group's Phase 1(a) Initial Report included a recommendation to eliminate the Transfer Confirmation and replace it with a Notification of TAC Issuance and a Notification of Transfer Completion. In its review of public comments and subsequent deliberations, the working group extensively discussed key concerns that were raised:

- Domains are important and valuable assets. It is important for registrants to have a genuine opportunity to approve or reject a transfer before the transfer takes place. In some cases, under the procedure recommended in the Initial Report, the transfer will have already taken place by the time the registrant has received the Notice of TAC Issuance and wants to take action to stop the transfer. This process takes agency away from the registrant. It increases the risk of a domain being stolen without the knowledge of the registrant, in particular where an unauthorized party has accessed the TAC to initiate a transfer that the registrant doesn't want.
 - Some working group members indicated that the working group could introduce a "fast undo" process during the discussion of Group 2 topics to more quickly reverse an unauthorized transfer. The working group was ultimately unable to reach agreement on a process for a "fast undo" process. Even if such a mechanism is recommended and ultimately implemented, transfer reversal is less desirable than the ability to reject a transfer before it occurs. Once the domain is transferred away, there has been a disruption. The DNS has changed, and service may have stopped. It requires a higher level of effort to remedy the situation, and more parties will need to be involved.
-

While there was disagreement among working group members about the utility of the Transfer Confirmation from a security perspective, it was understood that from a RNH perspective, elimination of the Transfer Confirmation results in a sense among some RNH's that they have lost an important element of agency in the process. Working group members acknowledged that in many cases of theft, the email and/or Registrar account is hacked, eliminating the value of the Transfer Confirmation, but this is not true in every case. If the TAC is stolen once it has been generated, the Transfer Confirmation can assist the RNH in stopping an unwanted transfer.

Some working group members advocated for an alternative means to provide additional agency to the registrant while reducing the overall maximum timeline of the transfer process. Specifically, they proposed that the Registrar of Record must be required to send a notification to the RNH once a TAC is requested. The RNH can respond to the notice by either accepting or rejecting the release of the TAC. If there is no response by a given period of time (a period of less than 5 days), the Registrar proceeds to issue the TAC. Those advocating for this approach noted that the proposal provides notice and opportunity to accept or reject at the moment the RNH is thinking about the transfer, shortly after they have requested the TAC.

Those opposing the proposal noted the following concerns:

- The proposal can stop the initiation of a transfer but does not stop a transfer that is pending. The TAC is vulnerable to theft once it is generated, and if the TAC is stolen once created, the RNH does not have a way to NACK the transfer as it does with the Transfer Confirmation.
- The proposal creates a need for system updates, process updates, and user education and may not fully satisfy those who want to keep the Transfer Confirmation. Therefore, the change is not worth the effort.

Ultimately, the working group did not come to an agreement to pursue this proposal further. As a default, the Transfer Confirmation will be maintained.

Recommendations: [#11](#), [#16](#), [#17](#), [#19](#)

Charter Question: Losing FOA

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?

Summary of Deliberations:

The CPH Tech Ops Group, “agreed that the requirement to notify the Registrant about a transfer request should be mandatory. As general business practices 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.”²¹

The working group agreed with Tech Ops that it is important to notify the RNH when a transfer is expected to take place and has recently taken place. The working group further supported the idea that given variations in Registrar business models and individual transfer scenarios, different secure means of communication may be appropriate for the provision of notifications.

Recommendations: [#11](#), [#19](#)

Charter Question: Losing FOA

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?

Summary of Deliberations:

The working group appreciates proposals received during the Public Comment period on the Phase 1(a) Initial Report and considered these proposals in its review of Public Comments. Please see [Public Comment review working documents](#) on the working group’s wiki for additional details.

Recommendations: N/A

²¹ Full text of the CPH Tech Ops proposal can be found in Annex B of the [TPR Final Issue Report](#).

Auth-Info Code Management

Charter Question: 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?

Summary of Deliberations:

The working group agreed that it should first establish clarity around the function and definition of the AuthInfo Code and ensure that terminology is clear before addressing specific security requirements. The working group used the following text on [ICANN.org](https://www.icann.org) as a starting point for discussion on the definition of the Transfer Authorization Code (TAC): “An Auth-Code (also called an Authorization Code, Auth-Info Code, or transfer code) is a code created by a Registrar to help identify the Registered Name Holder of a domain name in a generic top-level domain (gTLD). An Auth-Code is required for a Registered Name Holder to transfer a domain name from one Registrar to another.” The working group agreed that the term “identify” is inappropriate in this context, because the code does not verify identity in practice. Instead, the TAC is used to verify that the Registered Name Holder (RNH) requesting the transfer is the same RNH who holds the domain.

The working group considered that a number of different terms currently apply to the same concept, including AuthInfo Code, Auth-Info Code, Auth-Code, Authorization Code, and transfer code. None of these terms clearly describe the function of the code. The working group believes that it is clearer for all parties, and particularly the RNH, if a single term is used universally. The working group believes that “Transfer Authorization Code” (TAC) provides a straightforward description of the code’s function, and therefore should serve as the standard term in place of the alternatives.

Regarding the security of the TAC, the working group agreed that metrics could support deliberations on charter question b1. In particular, working group members were interested to see if there has been a change in the number of unauthorized transfers following adoption of the Temporary Specification for gTLD Registration Data. ICANN’s Contractual Compliance Department provided the working group with updated metrics regarding complaints received, which covered the periods both before and after the Temporary Specification went into effect.²² Contractual Compliance subsequently shared additional metrics that included the

²²Available at:

https://community.icann.org/download/attachments/181307054/Compliance_Transfer%20Data_presented%2029%20June%202021.xlsx?version=1&modificationDate=1638449700087&api=v2

“closure codes” associated with complaints about unauthorized transfers.²³ While the working group agreed that it is difficult to draw conclusions from the data, the working group noted that there was no notable increase in complaints following the date that the Temporary Specification went into effect.

The working group considered that in addition to examining metrics regarding past performance, it is important to consider future-state objectives for the TAC. The working group agreed that from this perspective, additional security features are appropriate to protect the RNH, drawing on elements of RFC 9154. In considering potential security enhancements, the working group considered the benefits of requiring these measures, while also taking into account usability considerations and operational impacts on contracted parties in implementing new requirements.

Recommendations: [#4](#), [#5](#), [#13](#)

Charter Question: Auth-Info Code Management

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?

Summary of Deliberations:

In considering this charter question, the working group focused on evaluating and defining specific roles and responsibilities of Registries and Registrars in the transfer process, noting that each party has an important role to play in the transfer process. While some working group members expressed the view that Registry management of the TAC would be more uniform, standardized, and transparent, others noted that standards will be set through policy and enforced by ICANN Contractual Compliance regardless of whether the authoritative holder is the Registry or Registrar; therefore, it is not clear why it would be better to have the Registry be the authoritative holder.

The working group ultimately did not identify a compelling reason to shift ownership of the TAC to the Registry and therefore determined that the Registrar must continue to generate the TAC, set the TAC in the Registry platform, and issue the TAC to the RNH or their designated

²³Available at:

https://community.icann.org/download/attachments/181307054/Compliance_Unauthorized%20Transfer%20Data%20Aug%202020-Sept%202021_presented%209%20November%202021.xlsx?version=1&modificationDate=1638449975000&api=v2

representative. The working group further agreed that the Registry should continue to verify the validity of the TAC and in addition, going forward, the Registry must verify that the TAC meets the syntax requirements specified in Recommendation 7. The working group provided recommendations to improve security practices with respect to the TAC to be implemented at the Registry. The working group has also recommended that the Registry enforce the 14-day validity of the TAC.

Recommendations: [#7](#), [#8](#), [#12](#)

Charter Question: Auth-Info Code Management

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?

Summary of Deliberations:

The working group agreed that the Transfer Policy should continue to require Registrars to issue the TAC to the RNH or their designated representative within a specified period of time following a request. While some working group members felt that the standard time frame for issuance of the TAC should be shorter than five calendar days, working group members noted that exceptions may be necessary to accommodate specific circumstances. The working group did not identify a compelling reason to change the five-day response timeframe but believes that it is appropriate to update the policy language to highlight that five calendar days is the maximum and not the standard period in which the TAC is to be issued. The working group also agreed that it is more clear to express the time frame in hours rather than calendar days.

Recommendations: [#6](#)

Charter Question: Auth-Info Code Management

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.)?

Summary of Deliberations:

The working group clarified its understanding that the Time to Live (TTL) is the period of time that the TAC is valid once the TAC has been created. The working group noted that there are no existing policy requirements regarding TTL. The working group believes that it is good security practice to have a standard TTL for the TAC, because old, unused TACs are vulnerable to exploitation.

The purpose of the standard Time to Live (TTL) is to enforce security around unused TACs (e.g., requested/received but not used), in a situation where the TAC may be stored in a registrant's email or other communications storage. The working group arrived at the conclusion that the TAC TTL must be no more than 14 calendar days / 336 hours and notes that a 14-day / 336 hour period is appropriate in order to accommodate transfer-related business processes associated with different registrar models.

The working group extensively discussed whether the Registry or Registrar should enforce the 14-day TTL and requested community input on this question through public comment on the Phase 1A Initial Report. The working group recommends enforcement by the Registry for the following reasons:

- For accuracy: If the sponsoring Registrar is required to expire the TAC by updating it to null, there is a possibility that at the time when the TAC is set to expire, either the Registrar or Registry systems have an outage (or there is a communication interruption). This means that the TAC expiration would be delayed until the transaction could be completed, opening a window for possible usage of a TAC that the sponsoring Registrar had deemed expired.
- For consistency: Having a centralized approach at the Registry allows prospective Gaining Registrars to know that every TAC will be expired at 14 days / 336 hours regardless of the sponsoring/provisioning Registrar.
- For security: Every TAC in a Registry has a maximum lifetime that is enforced consistently. This prevents the existence of any long-lived TAC, which could be used as part of an unauthorized or unintended inter-Registrar transfer.

With respect to 13.2, the working group acknowledged that there may be a variety of circumstances in which the Registrar of Record and the Registered Name Holder may want to mutually agree to reset the TAC to NULL prior to the end of the 14th calendar day. The working group included this language to ensure that Registrars are permitted to do so under relevant circumstances.

Recommendations: [#9](#)

Bulk Use of Auth-Info Codes

Charter Question: Bulk Use of Auth-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?

Summary of Deliberations:

As a general rule, the working group believes that one randomly generated TAC should be provided per domain name, because this is a good security practice (see Recommendation 13). The working group recognizes that for cases where multiple domains are being transferred, it would be more convenient to have a streamlined approach for requesting and using TACs. Some working group members suggested a carveout to the standard TAC requirements that would allow use of the same TAC for multiple domains if specific additional requirements were met to ensure security of the transaction. The working group did not agree on specific conditions under which this should be possible. Therefore, the working group is not making any recommendations with respect to exceptions for multi-domain transfers.

Recommendations: N/A

Charter Question: Bulk Use of Auth-Codes

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

Summary of Deliberations:

The working group carefully reviewed the TechOps proposal²⁴ and considered input from those involved in development of the proposal. The working group appreciated the expertise and relevant experience of those who developed the proposal and therefore considered it a logical starting point for discussion. The working group agreed, however, that it is important to consider (i) the range of views and interests that may not have been represented in the development of the proposal, and (ii) any new information or interests that have come to light since the development of the proposal. Therefore, in developing its recommendations, the working group deliberated on each of the charter questions, taking into account both the relevant elements of the TechOps paper as well as all other available information and inputs,

²⁴ Available in Annex B of the TPR [Final Issue Report](#).

including proposals submitted during the Public Comment period on the Phase 1(a) Initial Report.

Recommendations: N/A

Charter Question: Bulk Use of Auth-Codes

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?

Summary of Deliberations:

The working group does not believe that there should be any new policy requirements in this regard.

Recommendations: N/A

Wave 1, Recommendation 27

Charter Question: Wave 1, Recommendation 27

c1) How should the identified issues be addressed?

Summary of Deliberations:

The working group reviewed the Transfer Policy-related issues from Section 3.11 of the Wave 1 Report and noted seven (7) of the ten (10) “key issues” were relevant to the current phase (Phase 1(a)) of its work.²⁵ The working group reviewed and discussed these seven issues and has provided a response to each issue. The detailed responses can be found in Annex 8 of this report.

Recommendations: [#1](#), [#2](#)

²⁵ Key Issues 4, 6, and 7 related to Change of Registrant, and, accordingly, the working group agreed to discuss these issues during Phase 1(b) of its work.

Charter Question: Wave 1, Recommendation 27

c2) Can the FOA-related Transfer Policy issues (identified in paragraphs 5 and 9 of Wave 1 Report),²⁶ as well as the proposed updates to the Gaining and Losing FOAs, be discussed and reviewed during the review of FOAs?

Summary of Deliberations:

As noted above, the working group reviewed the seven key issues from Section 3.11 of the Wave 1 Report that are directly related to Group 1(a) of its work, including the issues related to the Gaining and Losing FOAs. The working group determined these specific issues are in scope for it to address during Group 1(a) and discussed and reviewed these issues during its plenary meetings. For the detailed responses on the key issues, please refer to Annex 8 of this report.

The working group noted many key issues alluded to terminology inconsistencies, which are the direct result of the EPDP Phase 1 recommendations. For example, EPDP Phase 1, Recommendation #5 provides an updated list of data elements to be collected by Registrars. Notably, the administrative contact field, which was a required data field under the 2013 RAA, is no longer a required data element for Registrar collection and subsequent processing. Because the administrative contact field is referenced many times within the Transfer Policy, the working group noted those references should be removed.²⁷ Similarly, the working group observed that the multiple references to “Whois” need to be updated.

Recommendations: [#1](#), [#2](#)**Charter Question: Denying Transfers (Inter-Registrar Transfers)**

²⁶ 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).

²⁷ Additional context from the working group’s discussion can be found in Annex 8 of this report.

h1) 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?

Summary of Deliberations:

The working group conducted a thorough review of the reasons for denying or NACKing a transfer and has provided a series of recommendations detailed below. Please see the rationale for each proposed change for additional information about why these updates are being recommended.

While discussing sections I.A.3.7 through I.A.3.9 of the Transfer Policy, the working group spent a significant amount of time considering I.A.3.7.5 and I.A.3.7.6 and the fact that in some cases, a domain is locked against inter-Registrar transfer for 60 days following the registration of the domain name or the transfer of the domain name to a new Registrar. Requirements regarding post-registration and post-transfer locks appear in some Registry Agreements and are reflected in corresponding Registry-Registrar Agreements. This practice is neither required nor prohibited in the Transfer Policy and is applied inconsistently across the industry.

The working group considered that this inconsistent practice may cause confusion among registrants and may lead to poor registrant experience. The working group supported establishing a standard set of requirements that apply across the industry. While some members also supported opportunities for opt-outs or flexibility in the requirements (for example a minimum lock period with an option to implement a longer lock period), the working group ultimately agreed that consistency needs to be maintained.

In the course of deliberations, the working group discussed three possible time periods for post-registration and post-transfer locks: 10 days, 30 days, and 60 days. Working group members supported maintaining consistency between the period that a transfer is prohibited following registration and following inter-Registrar transfer. Some working group members have advocated for establishing a “fast undo” process along the lines of the Expedited Transfer Reverse Process (ETRP) considered in Inter-Registrar Transfer Policy (IRTP) Part B Policy Development Process. The IRTP Part B Working Group ultimately did not adopt the ETRP proposal. The working group discussed the process of a “fast undo” or transfer reversal process but was ultimately unable to come to an agreement. Many working group members observed that registrars generally work together informally to undo an improper transfer, where appropriate, and introducing strict policy requirements around this may limit this ability.

Recommendations: [#18](#), [#20](#), [#21](#), [#22](#), [#23](#), [#24](#)

Charter Question: Denying Transfers (Inter-Registrar Transfers)

h2) 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?

Summary of Deliberations:

The working group reviewed the World Intellectual Property Organization’s (WIPO) [detailed comment](#) in response to the [Transfer Policy Status Report](#) and has noted two concerns involving a UDRP proceeding vis-à-vis the Transfer Policy. Specifically, WIPO has noted issues related to: (i) the locking of a domain name subject to a UDRP proceeding (in order to prevent an inter-Registrar transfer during the pendency of the proceeding),²⁸ and (ii) the implementation of a UDRP Panel’s order to transfer a domain name to a complainant.²⁹

Domain Name Locking

UDRP Rule 4(b) provides, in part, “Within two (2) business days of receiving the Provider’s verification request, the Registrar shall [. . .] confirm that a Lock³⁰ of the domain name has been applied. [. . .] The Lock shall remain in place through the remaining Pendency of the UDRP proceeding. [. . .].” Additionally, Paragraph I.A.3.8.1 of the Transfer Policy requires registrars to deny any requests for inter-registrar transfers during “a pending UDRP proceeding that the Registrar has been informed of.”

Within its recommendations, the working group has proposed to update the current Transfer Policy language to:

“The Registrar of Record MUST deny a transfer request in the following circumstances:

²⁸ For specific policy requirements, please see [UDRP Rule 1](#) (definitions of Lock and Pendency, respectively), [UDRP Rule 4\(b\)](#), and Paragraph I.A.3.8.1 of the [Transfer Policy](#).

²⁹ For specific policy requirements, please see [UDRP Section 4\(i\)](#), [4\(k\)](#), [UDRP Rule 16\(a\)](#).

³⁰ [UDRP Rule 1](#) defines Lock as “a set of measures that a Registrar applies to a domain name, which prevents at a minimum any modification to the registrant and Registrar information by the Respondent but does not affect the resolution of the domain name or the renewal of the domain name.”

- Pending UDRP proceeding that the Registrar has been notified of by the Provider in accordance with the UDRP Rules.”

The working group is proposing a slight refinement to the current text in an effort to clarify that a Registrar must deny inter-Registrar transfer requests that are received after the Registrar has been notified by a UDRP Provider of a UDRP Proceeding in accordance with the UDRP Rules.

In response to WIPO’s related concern that “the ambiguity associated with ‘locking’ a domain name has resulted in many improper domain name transfers,” the working group notes that the definition of Locking is part of the UDRP Rules, and, accordingly, appears out of scope for this working group to address. The working group does note, though, that the proposed updates to the Transfer Policy endeavor to make clear that Registrars are forbidden from implementing inter-Registrar transfer requests received following a notification from a UDRP Provider of a pending UDRP proceeding.

In the event a Registrar mistakenly or purposefully effects an inter-Registrar transfer during the pendency of a UDRP proceeding, this would be a clear violation of the Transfer Policy and should be referred to ICANN org Contractual Compliance for review. The working group will flag the definitional issue of “locking” with the Rights Protection Mechanisms (RPMs) Phase 2 Working Group, who will be closely reviewing the UDRP, and will be in a better position to determine if updates are needed.

Implementation of UDRP Panel Decisions

The working group also discussed WIPO’s noted concern regarding the reported refusal of some Registrars to effect a UDRP Panel’s decision to transfer a disputed domain name(s) to the Complainant.

Paragraph 4(i) of the UDRP provides that a UDRP Complainant may request the following remedies in its UDRP Complaint, “the cancellation of [a disputed] domain name or the *transfer* of [a disputed] domain name registration to the complainant.” (emphasis added). Paragraph 4(k) goes on to provide, in part, “if an Administrative Panel decides that [the disputed] domain name registration should be canceled or transferred, [the Registrar of Record] will wait ten (10) business days [. . .] before *implementing* that decision [to cancel or transfer the disputed domain name].” (emphasis added)

Registrar representatives within the working group noted various methods their companies use to implement UDRP decisions, including, for example, providing the AuthInfo Code to the

Complainant to effect the inter-Registrar transfer, setting up an account for the Complainant and transferring the name to the new account, et. al. The working group discussed that so long as the Registrar of Record effects the Panel's decision by allowing transfer of the domain name, the Registrar would be in compliance with the UDRP, and the working group was reluctant to recommend specific implementation restrictions.

The working group noted that a Registrar refusal to implement a UDRP Panel's decision to cancel or transfer the disputed domain name to the Complainant, absent official documentation of a court proceeding,³¹ would be a violation of the UDRP, and, accordingly, should be referred to ICANN org Contractual Compliance for review. The working group noted that it will refer this reported issue of UDRP decision implementation to the RPMs Phase 2 Working Group, as the working group believed the specific implementation around UDRP decisions to be out of scope for the Transfer Policy.

Recommendations: [#23](#)

³¹ See UDRP, Paragraph 4(k).

Annex 3 – Group 1(b) Charter Questions and WG Summary Deliberations

Annex 3 - Group 1(b) Charter Questions and WG Summary Deliberations

Change of Registrant

For context on this topic and the associated charter questions, please see pages 20-32 of the [Final Issue Report](#).

[Link](#) to TPR WG Charter.

Charter Question: Change of Registrant

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

Summary of Deliberations:

The working group discussed the following original goals associated with Change of Registrant:

- Standardization across registrars, creating a better/easier experience for registrants.
- Security improvements through ensuring the changes are authorized.
- Manage instances of domain theft/hijacking (especially with respect to the 60-day post Change of Registrant lock or inter-registrar transfer restriction).
- Consistent with Transfer Policy B.1. "In general, registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely."

In considering the question of whether the goals are still valid, the working group noted that a number of circumstances have changed since the IRTP-C working group completed its work:

- The registrar landscape had changed. From one perspective, security measures are more robust, especially as registrars work to meet obligations under GDPR.
- When Change of Registrant was drafted, email addresses were available in the public RDDS, which was a significant attack vector for domain name hijacking. This is no longer an issue.
- From one perspective, protection of registrant data against unwanted changes is even more important with GDPR, because the registrant cannot monitor the RDDS for such changes, and therefore needs to be informed by other means.

Working group members noted that while the [Transfer Policy Status Report](#) (PSR) provides a number of metrics, the data does not definitively provide an answer to whether the goals are being met, and specifically whether the policy requirements have an impact on security issues related to unauthorized activity. Survey results associated with the PSR and anecdotal information provide some evidence that adjustments to Change of Registrant are appropriate from a usability perspective, as the current requirements are perceived as confusing and cumbersome. The working group considered that it might be beneficial to recommend additional data collection and tracking in the future so that there are better metrics to leverage in future policy development related to the Transfer Policy.

Ultimately, working group members supported having Change of Registrant policy requirements in some form, but noted that changes were needed to those requirements. The recommended changes are noted in response to the additional charter questions below.

Recommendations: N/A

Charter Question: Change of Registrant

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

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?

Summary of Deliberations:

In initial discussions, some working group members expressed support for having two distinct policies, which those members noted may be a “tidier” approach.

The working group noted the two processes are distinct with two different purposes, histories, and sets of needs. They may, but often do not, happen at the same time. They should not be conflated. From this perspective, the working group noted it would be cleaner to keep the discussions separate.

The working group reviewed Section II of the Transfer Policy in its entirety to see if it was in need of changes, simplifications, or additional explanatory language. In addition to recommending a standalone policy, the working group recommended additional changes described in recommendations #25 and #26.

Recommendations: [#25](#), [#26](#)

Charter Question: Change of Registrant

d4) Survey responses and data provided by ICANN's Global Support Center indicate that registrants do not understand the 60-day lock and express frustration when it prevents them from completing an inter-registrar transfer. Does the 60-day lock meet the objective of reducing the incidence of domain hijacking? What data is available to help answer this question? Is 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?

Summary of Deliberations:

The working group reviewed the complaint metrics from ICANN Global Support and Contractual Compliance and, after discussing the metrics at length, has determined that the 60-day lock following a Change of Registrant appears to be a greater source of registrant frustration than proven registrant security. Furthermore, available data suggests that valid reports of domain hijacking are not as numerous as may be expected. For example, according to complaint metrics shared by ICANN Contractual Compliance, from September 2020 to October 2023 ICANN Compliance received:

- 205 complaints regarding Unauthorized Changes of Registrant
 - 169 were closed as invalid (without addressing with the Contracted Party)
 - 42 were sent to the Contracted Party
- 780 complaints regarding Unauthorized Inter-Registrar Transfers
 - 679 were closed as invalid (without addressing with the Contracted Party)
 - 88 were sent to the Contracted Party

The working group considered the number of complaints received by ICANN Compliance and sent to Contracted Parties to be relatively low, particularly when considering the vast number of domain names, changes of registrant, and inter-registrar transfers that occur worldwide. While most complaints of domain hijacking may be addressed internally with Registrars and are not escalated to ICANN Compliance, such issue tracking and reporting across Registrars may not be consistent or readily available and was not provided to the working group when requested.

Based on available data, it is not clear that the 60-day lock demonstrably reduces instances of domain hijacking. However, the working group noted that from the perspective of registrars, it is often difficult, if not impossible, to determine whether a registrant's email address or account login credentials have been compromised until after a complaint is received. While the 60-day lock temporarily prevents the registrant (and possible hijacker) from transferring the domain to another Registrar (also assuming the transfer lock was not opted-out of by the hijacker prior to the change of registrant), the lock does not prevent any initial hijacking of the registrant's credentials or account.

The working group discussed various ways that Registrars could address domain hijacking proactively rather than reactively, such as through additional requirements around accounts, control panels, and multifactor authentication. However, the working group noted that given the variety of Registrars and their business models, there is no one-size-fits-all security apparatus, and that flexibility should be given to Registrars to secure registrant data and accounts in ways that work best for them and their customers. That being said, the working group has proposed several recommendations within this Initial Report which would increase the security of inter-registrar transfers and help registrants catch and combat domain hijacking (such as required notifications to the RNH, instructions for how an RNH may reverse an invalid transfer, additional TAC requirements, implementation of a 30-day post-transfer restriction, etc.).

Recommendations: [#26.4](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

Rather than retaining the 60-day inter-registrar transfer lock following a Change of Registrant, the working group recommends eliminating it from the future Change of Registrant Data Policy (See Recommendation 26.4). The working group has noted several reasons why this 60-day post Change of Registrant inter-registrar transfer restriction/lock should be eliminated.

1. The working group discussed at length about the confusion and frustration from registrants around this restriction. Input from the Transfer Policy Survey, which was administered as part of the [Transfer Policy Status Report](#), also noted the inconsistency with which this lock is applied. Specifically, the language provides that registrars MAY offer an opt-out, but not all registrars choose to offer this, which ultimately leads to confusion among Registered Name Holders. Additionally, the working group noted that the common occurrence of a Registrar acting as the Designated Agent and opting out of the lock on behalf of the RNH, which is permitted in the COR policy, has rendered the security value of the 60-day lock meaningless or of negligible value.
 2. In recognition of the diminished security value of the 60-day post-COR lock, the working group instead recommends requiring a 30-day post inter-registrar transfer restriction, which is detailed in Recommendation 19. Barring an exception as described in Recommendation 19, domain names will remain at a registrar for 30 days following an inter-registrar transfer, allowing for any fraudulent changes to be unwound during this restriction period.
 3. The working group notes that the “clientTransferProhibited” status can be applied to a domain name at any time to prevent unwanted transfer. The 60-day COR lock is an unnecessary trigger, as such a lock is already available without additional requirements.
 4. The working group further notes that it has recommended a series of measures to increase the security of the Transfer Authorization Code (TAC) and reduce the risk that the TAC is obtained by an unauthorized party, as detailed in Recommendations 2-15. With the added security measures, the TAC becomes a stronger means to demonstrate that the TAC holder is an appropriate party to request the transfer, which makes the post-COR transfer restriction less important.
 5. The working group notes that when a Material Change to specified registration data elements occurs, the Registrar MUST send notifications to the Registered Name Holder further to Recommendation 27.
-

Recommendations: [#26.4](#), [#27](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

The working group believes that the widespread removal of public access to registrant data has indeed reduced the risk of hijacking. Working group members anecdotally observed that since 2018 and the redaction of registrant data from public lookup tools, there has been a noticeable drop in reports of domain data theft. This increased security of registrant data was a factor the working group considered when developing its recommendation to eliminate the 60-day lock from the future Change of Registrant Data Policy (See Recommendation 26.4).

Recommendations: [#26.4](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

The working group considered the 60-day lock's hindrance on legitimate domain transfers, including transfers resulting from corporate acquisitions, consolidations, and divestitures of large domain portfolios. In such circumstances, it is not uncommon that a Registrar transfer request follows a recent change of registrant, triggering the 60-day transfer lock much to the registrant's frustration. Having considered the concerns of registrants and the situations where it is necessary to readily transfer Registrars following a change of registrant, the working group recommends eliminating the 60-day lock from the future Change of Registrant Data Policy (See Recommendation 26.4).

Recommendations: [#26.4](#)

Charter Question: Change of Registrant

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

- There have been different interpretations of footnote 4 in the Transfer Policy, which states: “The Registrar may, but is not required to, impose restrictions on the removal of the lock described in Section II.C.2. For example, the Registrar will only remove the lock after five business days have passed, the lock removal must be authorized via the Prior Registrant’s affirmative response to email, etc.” Is the language in footnote 4 sufficiently clear as to whether registrars are permitted to remove the 60-day lock once imposed under the existing policy? If not, what revisions are needed?
- Should additional clarification be provided in Section II.C.1.3, which addresses how the information about the lock must be provided in a clear and conspicuous manner? Does the policy contemplate enough warning for registrants concerning the 60-day lock where they are requesting a COR?
- Should clarification be provided in Section II.C.2 that the option to opt-out is provided only to the Prior Registrant? For example, would the following revision be appropriate: “The Registrar must impose a 60-day inter-registrar transfer lock following a Change of Registrant, provided, however, that the Registrar may allow the Prior Registrant to opt out of the 60-day inter-registrar transfer lock prior to any Change of Registrant request.”?

Summary of Deliberations:

The working group recommends eliminating from the future Change of Registrant Data Policy the requirement that the Registrar impose a 60-day inter-registrar transfer lock following a Change of Registrant. Additionally, the working group recommends eliminating the option to opt-out of the 60-day lock, as there would no longer be a 60-day lock to opt-out of (See Recommendation 26.4). This elimination obviates the need to further clarify the 60-day lock and opt-out policy text.

However, the working group has identified other areas of the existing change of registrant policy (namely concerning notifications of a change of registrant) that it believes should be clarified and expanded on within the new standalone Change of Registrant Data Policy. The working group’s recommendations are provided below.

Recommendations: [#26.4](#), [#27](#), [#28](#)

Charter Question: Change of Registrant

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

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

Summary of Deliberations:

The working group reviewed the current definition of Change of Registrant at length. Ultimately, the working group generally agreed that the correct data fields were implicated, e.g, Registrant Name, Registrant Organization, and Registrant Email. The working group, however, noted that changes to these fields do not often equate to an actual Change of Registrant. Instead, the changes may only be to the same registrant’s data, i.e., a change to email, name change due to marriage, etc. Accordingly, the working group has recommended referring to these changes as Change of Registrant Data instead of Change of Registrant (See Recommendation 25).

The working group also discussed whether the addition or removal of privacy/proxy services constitutes a change of registrant data. It determined that a Change of Registrant Data is intended to reference the underlying registrant data on file with the Registrar and not necessarily what is always displayed in public RDDS lookups.

For example, if a registrant uses their Registrar’s privacy service to ensure their personal information in RDDS is not displayed publicly, and the registrant updates their email address on file with the Registrar, this would constitute a change of registrant data even though the RDDS record remains unchanged. Similarly, if a registrant decides to remove their Registrar’s privacy

service, but their underlying registrant data on file with the Registrar remains unchanged, this would not constitute a change of registrant even though the RDDS record may change to reflect the registrant's unmasked data.

The working group also acknowledged that some registrants choose to use privacy/proxy services outside of the sponsoring Registrar or their Affiliates (e.g., a registrant employing a trusted friend or business to manage the domain name on their behalf). In such circumstances, Registrars would not necessarily know that the registrant data provided to them belongs to a third-party P/P provider and not the true registrant. Ultimately, the working group decided that a change of registrant data refers to a material change of the registrant's name, organization, or email address on file with the Registrar, and not the addition or removal of known P/P services from the Registrar or its Affiliate. (See Recommendation 25.3).

Recommendations: [#25](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

In its discussions, the working group ultimately determined that privacy or proxy service data was not the focus of the Change of Registrant Data Policy, and updates related to P/P data are not considered a Change of Registrant Data.

Recommendations: [#25](#)

Charter Question: Change of Registrant

d11) 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?

Summary of Deliberations:

In its discussions, the working group ultimately determined that privacy or proxy service data was not the focus of the Change of Registrant Data Policy, and updates related to P/P data are not considered a Change of Registrant Data.

Recommendations: N/A

Charter Question: Change of Registrant

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

Summary of Deliberations:

In its discussions, the working group noted that there does appear to be overuse of the Designated Agent. While the Designated Agent function was critical to the early survival of wholesale Registrars, which interact regularly with resellers acting on behalf of registrants, today it is often used by resellers and Registrars to approve change of registrant requests for registrants who, at times unknowingly, delegate certain managerial responsibilities of their domain name data.

Recommendations: [#26](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

The working group believes that the Designated Agent role is not operating as intended and is also no longer fit for purpose, as the working group recommends eliminating from the future Change of Registrant Data Policy the requirement that the Registrar request and obtain confirmation from both the Prior Registrant and the New Registrant (see Recommendation 26.3).

Accordingly, without the need for a registrant to confirm a change of registrant data request (instead the RNH would be notified of any change they requested), the working group believes the Designated Agent role should be eliminated from the new standalone Change of Registrant Data Policy (See Recommendation 26.1). The working group also notes that while the Designated Agent function is no longer defined within the Change of Registrant Data Policy, this should not preclude or prevent Registrars from using third parties elsewhere if permitted by applicable policy.

Recommendations: [#26](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

The working group considered some alternative means to the Designated Agent, such as granting registrants the ability to waive some of their management rights directly to their Registrar. However, with the working group's removal of the confirmation requirement in lieu of additional notification requirements, the role of the Designated Agent remains unfit for purpose within the new Change of Registrant Data Policy (See Recommendation 26.1).

Recommendations: [#26](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

The working group recommends that the role and definition of Designated Agent is no longer fit for purpose, and therefore all references to Designated Agent must be eliminated from the future standalone Change of Registrant Data Policy (See Recommendation 26.1).

Recommendations: [#26](#)

Charter Question: Change of Registrant

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

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

Summary of Deliberations:

The working group recommends that the role and definition of Designated Agent is no longer fit for purpose, and therefore all references to Designated Agent must be eliminated from the future standalone Change of Registrant Data Policy (See Recommendation 26.1).

Recommendations: [#26](#)

Charter Question: Change of Registrant

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

Summary of Deliberations:

In its discussions, the working group found that the current requirement of receiving confirmation from both the prior registrant and new registrant before implementing a change of registrant presented data protection concerns which necessitated changes. It was determined that this confirmation was a data processing activity without true purpose, and that if confirmation is required it can be assumed from the registrant’s act of updating their data in the first place. Further, the confirmation requirement is often a confusing or disrupting event for registrants rather than presenting the intended benefit of notifying them of the update.

Recommendations: [#26](#)

EPDP Phase 1, Recommendation 27, Related to Change of Registrant**Charter Question: EPDP Phase 1, Recommendation 27, Related to Change of Registrant**

e1) How should the identified issues be addressed?

Summary of Deliberations:

The working group reviewed the two key issues from Section 3.11 of the Wave 1 Report that are directly related to Group 1(b) of its work, including the issues related to the Change of Registrant. The working group determined these specific issues are in scope for it to address during Group 1(b) and discussed and reviewed these issues during its plenary meetings. For the detailed responses on the key issues, please refer to Annex 8 of this report.

Recommendations: N/A

Charter Question: EPDP Phase 1, Recommendation 27, Related to Change of Registrant

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

Summary of Deliberations:

The working group reviewed Section II.B.1 of the Transfer Policy, which was identified in paragraph 6 of the Wave 1 report as needing further clarification. While the working group recommends eliminating Section II.B “Availability of Change of Registrant” from the future standalone Change of Registrant Data Policy (See Recommendation 26.2), the working group also clarified that a change of registrant data does not necessarily entail a change to the data that is displayed publicly in RDDS (See Recommendation 25.3). For further details, please refer to Annex 8 of this report.

Recommendations: [#25](#), [#26](#)

Annex 4 – Group 2 Charter Questions and WG Summary Deliberations

Annex 4 - Group 2 Charter Questions and WG Summary Deliberations

[Link](#) to TPR WG Charter.

Transfer Emergency Action Contact (Inter-Registrar Transfers)

For context on this topic and the associated charter questions, please see pages 33-37 of the [Final Issue Report](#).

Charter Question: Transfer Emergency Action Contact (Inter-Registrar Transfers)

f1) Is additional data needed to support evaluation of the effectiveness of the TEAC mechanism? If so, what data is needed?

Summary of Deliberations:

To support discussion on whether adjustments may be needed to the TEAC communication channel and associated policy requirements, the working group first reviewed relevant information in the Transfer Policy Status Report. In particular, the working group considered responses to the Registrar survey that describe pain points with respect to the TEAC communication channel. The working group noted the relevance of specific comments as they relate to charter questions under this topic. Specifically:

- Survey responses regarding the 4-hour time frame for Registrars to provide an initial, non-automated response to communications via the TEAC communication channel. The working group considered these comments during deliberations on Charter Questions f2 and f3.
- Comments regarding the need for more accountability in reaching a resolution after the issue has been raised through the TEAC communication channel. The working group considered these comments during deliberations on Charter Question f4.

The working group reviewed metrics in the [Transfer Policy Status Report](#)³² reflecting ICANN Contractual Compliance Complaints received between August 2017 and July 2018 with the Transfer Complaint Category “Transfer Emergency Action Contact.” The working group noted that there were a total of three complaints in the relevant category during that period.

³² See p. 30 of the [Transfer Policy Status Report](#).

The working group requested that ICANN’s Contractual Compliance department provide more recent metrics regarding complaints, which might help to determine if there are notable trends in the number of complaints. ICANN’s Contractual Compliance department provided the working group with metrics covering the period from 1 September 2020 to 31 December 2022. During that period, there were five Compliance cases that were validated and confirmed to refer to TEAC obligations described in the Transfer Policy. Compliance further shared with the working group that in those five cases, the reported issue was that the TEAC did not provide an initial response within the required 4-hour time frame. In all cases, there was a time zone difference between the involved parties. All cases were closed after the reported Registrars took corrective action, such as allocating 24x7 staffing to the TEAC communication channel. The working group made note of this additional input in discussions related to charter questions f2 and f3.

The working group observed that survey responses and Contractual Compliance metrics provide some insight into pain points but also noted that additional information would be useful to support an assessment of the TEAC mechanism. In early input on the charter questions provided by Stakeholder Groups/Constituencies, the following data points were identified as potentially useful:

- Number of times TEAC communication channel is used
- Modes of contact to TEAC, and whether these are satisfactory
- Steps taken before contacting TEAC
- Quality of initial response by TEAC
- Whether the timeframe for response is satisfactory
- Circumstances prompting use of TEAC
- Number of cases where there are problems associated with use of the TEAC, including abuse of the TEAC communication channel
- Circumstances of issues experienced with the TEAC
- Type of resolution of case raised through TEAC
- Level of satisfaction with final resolution

The working group further recalled that the working group charter identified the following additional metrics as potential data points to measure whether policy goals are achieved:

- 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”
-

The working group agreed that the decentralized nature of the TEAC mechanism makes it difficult to consistently track information about utilization of the TEAC communication channel and that in practice, potentially useful data points are not readily available. The working group considered that if a centralized system of record were to be used for TEAC communications in the future, it would be easier to track certain information, such as the total number of TEAC requests and the timeframe for initial response. As discussed in the working group's response to Charter Question f5, the working group decided not to recommend that ICANN pursue a centralized system of record for TEAC communications.

The working group considered whether to recommend that either Registrars or ICANN must track and analyze additional information regarding the TEAC communication channel to support future review of the mechanism. After discussing the reported low volumes of occurrence, the working group concluded that any such effort would be resource intensive and logistically difficult given the decentralized nature of the mechanism.

The working group concluded that survey results, metrics from ICANN's Contractual Compliance department, and anecdotal input from Registrar and Registry representatives in the working group provide a sufficient basis to respond to the Charter Questions regarding the TEAC mechanism.

Recommendations: N/A

Charter Question: Transfer Emergency Action Contact (Inter-Registrar Transfers)

f2) 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?
- 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?

f3) 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?

Summary of Deliberations:

The working group reviewed survey responses from the Transfer Policy Status report and concerns raised by the Transfer Policy Scoping Team with respect to the 4-hour time frame for a Gaining Registrar to provide an initial response to communications via the TEAC communication channel. Registrar representatives in the working group confirmed that the burden of this requirement can be especially acute when Registrars are working across time zones and languages and for Registrars with smaller teams.

Registrar representatives in the working group further observed that the consequences of failing to respond to a TEAC communication within 4 hours can be significant. As detailed in Section I.A.6.4 of the Transfer Policy, a Losing Registrar may ask the Registry Operator to “undo” the transfer in cases where the Gaining Registrar fails to respond within the 4-hour time frame. Registrar representatives in the working group have observed situations where a Losing Registrar reaches out to a TEAC in the middle of the night or during a holiday period in the Gaining Registrar’s country, understanding that the TEAC may be slower to respond than usual. The Losing Registrar takes this action with expectation that the TEAC may miss the 4-hour deadline, enabling the Losing Registrar to ask the Registry Operator to “undo” the transfer. While the frequency of such occurrences is unknown, the working group agreed that such misuse of the TEAC communication channel should be a factor in reconsidering the timeline.

In light of concerns about the tight timeline for initial response to a TEAC request and significant consequences for missing the deadline, some working group members suggested that there should be a different set of requirements when two Registrars are based in distant time zones. Other working group members suggested that the consequences for missing the timeline should be less severe than a transfer “undo.” The working group did not come to agreement on either of these proposals.

Ultimately, the working group agreed that a longer timeframe for initial response, universally applied, is the simplest solution to addressing the concerns raised. The working group noted that the RAA provides a 24-hour deadline for Registrars to provide an initial, non-automated response to reports of illegal activity, although final resolution of the underlying issue may take longer. The working group observed that communication to a TEAC could be considered an analogous use case and agreed that a 24-hour time frame for initial response is acceptable for

handling emergencies, while addressing concerns raised by Registrars about the operational impacts of TEAC requirements and associated risks of misuse.

Recommendations: [#29](#)

Charter Question: Transfer Emergency Action Contact (Inter-Registrar Transfers)

f4) 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?

Summary of Deliberations:

The working group reviewed Section 1.A.4.6.2 of the Transfer Policy and agreed with the Scoping Team’s assessment that “timely manner” and “within a reasonable period of time following the alleged unauthorized loss of a domain” are open to different interpretations and need to be better defined. The working group agreed that clear policy language will ensure that all Registrars have a common understanding of the expected parameters within which the TEAC communication channel may be used.

The working group considered a suggestion from RrSG early written input that the timeframe for an initial communication to the TEAC should be aligned with the point in time at which the Registrar is made aware of the alleged unauthorized transfer, rather than the alleged unauthorized loss of a domain. The working group agreed that it is difficult to validate when a Registrar has become aware of an unauthorized transfer, and determined that it is more appropriate to keep the objective point of reference currently included in the policy.

The working group considered whether it may be appropriate to define a specific period of time after which the TEAC may no longer be used. The policy could state, for example, “Communications to a TEAC must be initiated in a timely manner, within x days following the alleged unauthorized loss of a domain.” Some working group members provided the perspective that if an extended period of time passes following alleged unauthorized loss of a domain and the registrant fails to notice and alert the Registrar, this may be an indication that the situation is not a true emergency, and therefore TEAC is not the appropriate channel for resolution. Other working group members expressed that there may be extenuating circumstances in which a long period of time has passed following the alleged unauthorized loss

of a domain but resolution is an emergency nonetheless. It was noted that the definition of an “emergency” can be subjective and dependent on circumstances.

The working group agreed that the most appropriate path forward is to set a clear expectation for a “reasonable period of time” while also providing an opportunity to use the TEAC communication channel after a longer period under extenuating circumstances. In considering how to define “reasonable period of time,” the working group noted that recommendations 16 and 17 provide for a 30-day transfer restriction following registration or an inter-Registrar transfer. The purpose of these recommendations is to provide an opportunity for the registrant and Registrar to identify and act on unwanted or unauthorized activity before a subsequent inter-Registrar transfer can take place. The working group agreed that a 30-day period is also an appropriate standard timeframe limit for the registrant and prior sponsoring Registrar to identify and initiate action on an emergency associated with a transfer.

In reviewing survey responses included in the Transfer Policy Status Report, the working group identified a second issue to consider under this charter question. The policy specifies a timeframe by which the TEAC must provide an initial, non-automated response, but in many cases, additional steps are required to resolve the issue raised through the TEAC communication channel. Some working group members and survey respondents indicated that more structure and guidance is needed regarding the expected timeframe for reaching a final resolution on an issue raised through the TEAC communication channel. Currently, the policy has no such requirements.

Registrar representatives in the working group shared that in some cases, a TEAC will provide a timely initial response that is not substantive, but will then take an extended period of time to follow up and work towards resolution of the issue. Some Registrar representatives expressed concern that absent any policy requirements, there is no penalty for a Registrar who delays or fails to follow through on resolution of an emergency request.

Working group members considered whether it could be possible to define a deadline or set timeframe by which resolution of an issue raised through the TEAC communication channel must be resolved. Working group members considered that there may be many different types of issues raised through the TEAC communication channel and different resolution paths. Absent data on the types of issues that Registrars handle through the TEAC communication channel and standard timeframes for resolution, it is difficult to set standard requirements and deadlines. In addition, it was noted that rigid requirements might result in a Registrar being penalized for missing a deadline, even though the Registrar is working diligently to resolve a particularly complex issue.

Ultimately, the working group determined that it is not appropriate to set fixed deadlines for resolution of an issue raised through the TEAC communication channel. Instead, the working group agreed that there should be requirements for greater transparency and accountability with respect to resolution of issues raised through the TEAC communication channel. Namely, the working group agreed that the Gaining Registrar must provide regular updates to the Losing Registrar who initiated the TEAC request and must demonstrate progress towards resolution of the issue as detailed in Recommendation 31.

Recommendations: [#30](#), [#31](#)

Charter Question: Transfer Emergency Action Contact (Inter-Registrar Transfers)

f5) 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?

Summary of Deliberations:

The working group observed that the paper trail associated with telephone communications may be less robust than records associated with other forms of communication, such as email. This limited paper trail may make it more difficult to verify the sequence of events associated with a TEAC communication when the Losing Registrar:

- Reports to ICANN Contractual Compliance Department that the Losing Registrar called the Gaining Registrar’s TEAC and the TEAC did not pick up the call or call back within the required timeframe.
- Requests that the Registry Operator “undo” a transfer because the Losing Registrar called the Gaining Registrar’s TEAC and the TEAC did not pick up the call or call back within the required timeframe.

It was noted that while it is technically possible to extract call logs to use as evidence, this type of investigation can be time-consuming and labor-intensive in practice. The working group

observed that it may be beneficial to establish a consistent means of documenting the initial communication exchange involving the TEAC communication channel.

The working group considered the potential merits of establishing an “authoritative system of record” for TEAC communications. Working group members noted, for example, that ICANN could explore whether the Naming Services Portal could be modified to allow Registrars to send, receive, and respond to TEAC communications through the portal. Such a system could potentially provide a clear record of communications with associated timestamps. An additional benefit would be the possibility of collecting and tracking metrics about use of the TEAC in the aggregate across Registrars. Some working group members envisioned a model in which one Registrar could initiate a TEAC request in the system, which would transmit the request to another Registrar’s TEAC via the communications channel of the recipient’s (email, phone, text, etc), while capturing records centrally.

Some Registrar representatives in the working group opposed rigid requirements regarding the method of contact by which TEAC communications occur. From this perspective, when handling an emergency, it is beneficial to have flexibility. Working group members further noted that a centralized system of record could be costly to develop and burdensome for Registrars to adopt. While it is unknown how often Registrars contact one another via the TEAC communication channel, there is anecdotal evidence that the numbers are low. Some working group members expressed that if TEAC communications are limited in number, such a transition to an authoritative system of record may not be worth the effort. Working group members also noted that a centralized system creates a single point of failure, which may be undesirable when handling emergency situations.

The working group sought alternatives that would maintain flexibility for Registrars to continue to use the phone, where appropriate, while also creating a more robust paper trail. The working group agreed that Registrars should have the discretion to use the method of communication they choose, including text messages and phone calls, but if the initial contact occurs by means other than email, Registrars must supplement this communication with an email exchange. This email exchange is comprised of:

1. The first email that the Losing Registrar sends to the Gaining Registrar’s TEAC, and
2. The initial response that the TEAC provides.

The working group considered whether it would be desirable to copy ICANN org and the Registry on the initial email exchange. It was noted that doing so might create the expectation that ICANN org or the Registry is taking action on the exchange, when in fact, they are not. It was also noted that from a data privacy standpoint, it is likely inappropriate to copy additional

parties on emails that contain personally identifiable information without a clear purpose for those parties to be collecting and retaining the information.

ICANN’s Contractual Compliance department and Registry representatives noted that org and Registries have due diligence processes already in place to address reports that a Gaining Registrar has failed to respond to a TEAC request within the required timeframe. An email copy is not expected to eliminate the need for these due diligence steps, and therefore org and Registries saw limited utility in being copied.

In light of these considerations, the working group determined that the Registry and ICANN org should not be copied on emails by default.

Recommendations: [#32](#)

Charter Question: Transfer Emergency Action Contact (Inter-Registrar Transfers)

f6) 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 f6 iii., 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.

f7) 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?

Summary of Deliberations:

Following discussion with members of the working group, ICANN's Global Domains & Strategy (GDS) Team looked into the issues described in Charter Questions f6 and f7 and was able to update their internal process to address the issue. Specifically, announcements of changes to Registrar contacts, which are sent on a weekly basis, now include all updates to TEAC contacts. Registry representatives from the working group have confirmed that this issue is now resolved without further discussion or intervention from the working group.

Recommendations: N/A

Transfer Dispute Resolution Policy

For context on this topic and the associated charter questions, please see pages 37-43 of the [Final Issue Report](#).

Charter Question: Transfer Dispute Resolution Policy

g1) 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?

Summary of Deliberations:

The working group noted the limited data available to review the TDRP; however, the working group reviewed what was available, including published TDRP decisions and ICANN Compliance data related to the TDRP. In its review of this data, the working group noted that there is difficulty in making conclusions based on the available data since the majority of transfer-related disputes are handled outside of the TDRP, i.e., via the TEAC communication channel, via informal resolution between registrars, or the court system.

The working group noted that the small number of cases does not, alone, indicate that the TDRP is an ineffective mechanism for resolving disputes between registrars in cases of alleged violations of the Transfer Policy. The TDRP was designed to address violations of the Transfer Policy. The TDRP was not designed to address all tangential transfer issues of disgruntled registrants; for example, the TDRP cannot and was not designed to address instances of domain theft, human error, business disputes, etc.

In its analysis of the data, the working group noted that while the TDRP filings were limited, the working group felt the available data was sufficient to demonstrate the TDRP is an effective mechanism for resolving the types of disputes it was designed to address: alleged violations of the Transfer Policy.

Recommendations: N/A

Charter Question: Transfer Dispute Resolution Policy

g2) 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?

Summary of Deliberations:

The working group reviewed multiple sources as it formed its response to this question. Specifically, the working group reviewed (i) the text of the TDRP relating to the documentary information required to be provided by filing and responding parties, (iii) the specific cases published on the TDRP providers' websites, (iii) the existing information ICANN org provides on its web pages related to transfer disputes and transfer-related issues.

The working group noted that the TDRP's evidentiary requirements seem sufficiently clear; however, the working group further noted that the limited amount of TDRP filings makes it difficult to identify any clear pattern of deficiencies or problems with the current text related to required documentation. Accordingly, the working group did note that this specific question may need to be reviewed in the future to assess whether additional TDRP decisions indicate any gaps where further context could be provided.

Lastly, the working group noted that the information provided by complainants and respondents would likely be updated pursuant to EPDP Phase 1, Recommendation 27, and, to that end, any updates must be drafted clearly to aid the understanding of providers, parties, and panelists.

Recommendations: N/A

Charter Question: Transfer Dispute Resolution Policy

g3) 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?

Summary of Deliberations:

The working group agreed that the Transfer Policy Dispute Resolution (TDRP) is currently insufficient in one important respect: it is exclusively for use by registrars and remains unavailable to domain name registrants.

i. In reviewing this question, the working group reviewed the prior determination of the IRTP Working Group Part D. Following extensive discussion, the IRTP WG Part D determined the TDRP should not be made available to registrants. Specifically, IRTP WG D, in its Final Report, provided the following recommendation, “The WG recommends not to develop dispute options for registrants as part of the current TDRP.” That Working Group ultimately determined that allowing registrants to access the TDRP directly could potentially (i) overload the TDRP and lead to abusive filings, (ii) result in complications based on the TDRP payment schedule (the “loser pays” model), and (iii) pose an issue for documentary evidence, as the relevant registrars are generally in possession of the evidence needed to file a TDRP, not the registrant.

The working group discussed the above factors and also noted that many registrant concerns and issues with unauthorized inter-registrar transfers fall outside the limited scope the TDRP is designed to address. For example, a bad actor may compromise a registrant’s account, update contact details, retrieve the Transfer Authorization Code (TAC), and transfer a domain name to another registrar without the authorization of the registrant. This type of transfer may technically comply with the Transfer Policy, provided the required steps are followed, even though the domain name was compromised prior to the transfer.

With this in mind, the working group observed that it would be beneficial and timely for the GNSO to further research the advantages and disadvantages of creating a dispute resolution mechanism for registrant filers. At a minimum, the working group believes the option of rethinking registrant access to the TDRP should be further explored. The working group also recommends that the GNSO also explore, via an Issues Report or similar method, the pros and cons of a stand-alone dispute resolution mechanism for registrant filers. Specifically, the working group recommends exploring the feasibility of creating a narrowly-tailored dispute resolution mechanism similar to the Uniform Domain Name Dispute Resolution Policy, whereby a registrant pays a filing fee, provides documentary evidence showing an improper transfer has

occurred, and a neutral panelist makes a determination whether to transfer a domain name or deny a complaint.

ii. As noted above, the working group discussed the pitfalls and disadvantages provided by the IRTP WG Part D with respect to registrant access to the TDRP. The working group noted that if a registrant believes an improper transfer has taken place, and its previous registrar of record is either unresponsive or unable to resolve the issue informally and/or the previous registrar is unwilling to file a TDRP complaint, the registrant is left with unfavorable options. The registrant could choose to file a complaint with ICANN compliance; however, ICANN compliance does not have the authority to reverse a transfer. The registrant could also choose to go to court; however, that option can be prohibitively expensive, especially compared to the cost of filing a TDRP complaint.

For these reasons, and the reasons noted in section (i), the working group is recommending the GNSO request an Issues Report on registrant dispute options for improper domain name transfers.

Recommendations: [#33](#)

Charter Question: Transfer Dispute Resolution Policy

g4) Are requirements for the processing of registration data, as specified in the TDRP, compliant with data protection law?

g5) 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?

Summary of Deliberations:

In reviewing this charter question, the working group reviewed the documentary evidence that is processed during the course of a TDRP proceeding, including data points that are provided by the Complainant to the Provider, the Respondent to the Provider, and the Provider to the Panelist.

The working group noted that some evidentiary requirements need to be updated based on outdated language that needs to change as a result of EPDP Phase 1, Rec. 27. The working group has provided draft updates to the TDRP in Annex 9. For further information, please refer

to Annex 8, where the working group’s comprehensive review of the Rec. 27 updates is contained.

Recommendations: N/A

ICANN-Approved Transfers

For context on this topic and the associated charter questions, please see pages 37-43 of the [Final Issue Report](#).

Charter Question: ICANN-Approved Transfers

i1) 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?

Summary of Deliberations:

*Note: the challenges referenced in Section 3.1.7.2 of the [Final Issues Report](#) are provided below for ease of reference:

“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 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.” - pp. 50-51 of [Final Issues Report](#)

In discussing this topic, the working group wished to clarify the various types of bulk transfers in order to elucidate the recommendation text. Specifically, Section I.B.2 of the Transfer Policy

refers to “full portfolio transfers,” which the working group described as a Registrar transferring all of its domain names under management (due to termination of a Registrar Accreditation Agreement) or all of its domain names within a specific TLD(s) (due to termination of a Registry Registrar Agreement). Full Portfolio Transfers are distinct from partial bulk transfers, which the working group describes as “Change of Sponsorship”). The working group chose to use these references, Full Portfolio Transfers and Change of Sponsorship within this report to avoid confusion.

The working group deliberated the required fee in I.B.2 at length, and Registry representatives noted that the fee is in recognition of the administration and coordination required to implement a full portfolio transfer. Accordingly, the working group agreed that in the case of an involuntary transfer, the Registry may charge a fee, but the Registry may not charge a fee in the event of an involuntary full portfolio transfer. The working group noted the challenges in securing a Gaining Registrar for involuntary full portfolio transfers, described by ICANN org and agreed the fee should be waived in these instances.

In discussing this question, the working group reviewed the entirety of the policy language in I.B and noted that the language related to fees was outdated. The working group discussed at length the possibility of an updated process, noting that the DNS landscape has changed significantly with the addition of many more Registry Operators and TLDs than when the policy language in 1.B was first introduced. Recommendations #34 - #39 propose a new process for the fee associated with voluntary full portfolio transfers. The working group retained the current domain name ceiling of 50,000 names and the current fee of \$50,000; in other words, a potential fee is triggered when the full portfolio transfer involves 50,000 or more domain names. The working group, however, introduced the concept of a collective fee, which means the fee across all involved registry operators cannot exceed \$50,000 total. In other words, the fee is calculated by the total number of domain names involved in the full portfolio transfer, instead of per TLD. This is explained in more detail in the recommendation text of #34 - #39, which should be considered collectively.

Recommendations: [#34](#), [#35](#), [#36](#), [#37](#), [#38](#), [#39](#)

Charter Question: ICANN-Approved Transfers

i2) 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?

Summary of Deliberations:

During the public comment period on Preliminary Issue Report, all three commenters recommended the topic of ICANN-approved transfers be further examined by the eventual working group. Accordingly, this charter question was added to the working group's charter.

Specifically, commenters raised concerns about the current scope of ICANN-approved bulk transfers being very limited, and requesting an eventual working group 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."

The working group received the following early input related to this topic:

RySG: In this context, the RySG is distinguishing a "voluntary bulk transfer" from "near-simultaneous, traditional inter-registrar transfers" by assuming that the former is intended to mean "a transfer that does not include term extension". The RySG supports an expansion of a RO's ability to provide a voluntary bulk transfer capability.

However, the RySG does not support enforced uniformity of voluntary bulk transfer across all ROs. The RySG believes that an RO should be able to use its bulk transfer capability as a competitive differentiator. The RySG supports an approach to voluntary/partial bulk transfers (i.e. multi-domain, batch-oriented transfers without term extension) that simply involves tri-party agreement between RO, Sponsoring Registrar, and Gaining Registrar.

RrSG: While this would be desirable for registrars, what is the frequency of these transfers? Is it common enough that a uniform set of rules should be established? This will require process changes for Registries, so the cost to make the changes should be justified through common usage. With this additional information, the RrSG can provide better feedback.

The working group was presented with the below poll question to consider the future approach:

Should the scope of voluntary bulk transfers, including partial bulk transfers, be expanded and/or made uniform across:

1. all Registry operators (via an update to the Transfer Policy)
OR
2. all Registry operators who offer the BTAPPA (via recommended updates to the BTAPPA)

Working group member noted:

- In cases where one Registry uses BTAPPA but another does not, that can be a barrier to transferring (e.g. a normal transfer of 20,000 names can be expensive and inconvenient)
- A uniform approach can also include built-in flexibility.
- The [BTAPPA boilerplate](#) language could potentially be loosened to be more widely accessible while remaining a voluntary service.
- In some situations, a Registrar's agent (a reseller) may need to change the sponsoring registrar due to data privacy concerns, and there is currently not the ability to do this

The working group ultimately agreed to expand the BTAPPA to all Registry Operators via the Transfer Policy, agreed to expand the BTAPPA to Registrar agents to allow for greater flexibility (noting that the Registrar is ultimately responsible for compliance with the Transfer Policy), and the working group conducted a comprehensive review of the [BTAPPA boilerplate](#) and developed policy recommendations with that as a model.

Recommendations: [#40](#), [#41](#), [#42](#), [#43](#), [#44](#), [#45](#), [#46](#), [#47](#)

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

Charter Question: Recommendation 27 Report (Inter-Registrar and Inter-Registrant Transfers)

j1) How should the identified issues be addressed?

Summary of Deliberations:

The working group conducted a detailed analysis of the issues identified in the Wave 1, Recommendation 27 Report, and its analysis can be found in Annex 8. Where updated language is recommended, the recommendation references have been included below.

Recommendations: [#1](#), [#2](#), [#15](#), [#25](#), [#26](#)

Charter Question: Recommendation 27 Report (Inter-Registrar and Inter-Registrant Transfers)

j2) 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?

Summary of Deliberations:

The working group determined that yes, the TDRP-related issues from the Wave 1, Recommendation 27 Report could be reviewed during the working group's review of the TDRP. The working group provided its analysis in Annex 8 and proposed updated language for the TDRP in Annex 9.

Recommendations: N/A

Charter Question: Recommendation 27 Report (Inter-Registrar and Inter-Registrant Transfers)

j3) 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?

Summary of Deliberations:

The working group did not identify any additional issues.

Recommendations: N/A

Charter Question: Recommendation 27 Report (Inter-Registrar and Inter-Registrant Transfers)

j4) Should these issues, or a subset of these issues, be resolved urgently rather than waiting for the respective PDP Working Group?

Summary of Deliberations:

The working group did not identify any issues that needed urgent resolution.

Recommendations: N/A

Annex 5 – Working Group Approach

This section provides an overview of the working methodology and approach of the working group. The points outlined below are meant to provide the reader with relevant background information on the working group’s deliberations and processes and should not be read as representing the entirety of the efforts and deliberations of the working group.

Project Plan

The working group’s first deliverable was to provide the GNSO Council with a Phase 1(a) project plan. To develop the project plan, the leadership team sought input from members about the sequence in which to address topics and the amount of time each topic would take to discuss. This input was used to develop the [project plan](#), which was delivered to the GNSO Council for its consideration during the [22 July 2021](#) Council meeting.

As deliberations progressed, the working group agreed that it was important to examine all elements of the security model for domain name transfers in a holistic manner as part of its Phase 1 deliberations. The working group determined that the topic denying (NACKing) transfers should be addressed in Phase 1(a) rather than Phase 2 as originally included in the charter. As a result, the working group leadership team submitted a Project Change Request to the GNSO Council, which Council [adopted](#) on 16 December 2021. The expanded scope did not impact its target delivery dates to which the working group committed.

During the course of its Phase 1(b) work, the working group recognized that certain Phase 2 topics must be addressed before Phase 1 recommendations could be fully developed. Specifically, the working group observed that the charter questions related to the Transfer Dispute Resolution Policy (TDRP) and the Transfer Emergency Action Contract (TEAC), two Phase 2 topics, were dependencies for both Phase 1(a) and Phase 1(b) recommendations. As a result, the leadership team prepared a [Project Change Request \(PCR\)](#) to update its work plan to (i) consolidate all work into a single phase and (ii) change the order in which topics were to be considered. The GNSO Council [approved](#) the PCR during its meeting on 16 February 2023. Because the PDP was initially chartered in two phases, as a consequence of the approved PCR, the [charter](#) was updated to include minor revisions to remove references to phases.

Early Community Input

In accordance with GNSO policy development process requirements, the working group [sought written input](#) on the charter topics from each Supporting Organization, Advisory Committee and GNSO Stakeholder Group / Constituency. The input received was incorporated into the working group’s deliberations as each topic was discussed. Since all groups that provided

written input also had representative members or appointed subject matter experts in the working group, those members were well positioned to respond to clarifying questions from other members about the written input as it was considered.

Methodology for Deliberations

The working group began its deliberations for Phase 1(a) on 14 May 2021. The working group agreed to continue its work primarily through conference calls scheduled weekly, in addition to email exchanges on its mailing list. The working group held sessions during [ICANN71](#), [ICANN72](#), [ICANN73](#), [ICANN74](#), [ICANN75](#), [ICANN76](#), [ICANN77](#), [ICANN78](#), [ICANN79](#), and [ICANN80](#). These sessions provided an opportunity for the broader community to contribute to the working group's deliberations and provide input on the charter topics being discussed.

All of the working group's work is documented on its [wiki workspace](#), including its meetings, mailing list, meeting notes, deliberation summaries, draft documents, background materials, [early input](#) received from ICANN org, and input received from ICANN's Supporting Organizations and Advisory Committees, including the GNSO's Stakeholder Groups and Constituencies.

To develop the content included in the Initial Report, the working group progressed through the charter questions by topic, following the sequence established in the project plan. Because the topics are closely interrelated, the working group took an iterative approach to producing and reviewing draft responses to charter questions and draft preliminary recommendations to ensure that the full package of outputs was coherent and comprehensive.

To ensure that all groups represented in the working group had ample opportunity to provide input to the deliberations, the leadership team opened each working group meeting with an invitation for members to step forward and provide any updates about discussions happening within their Supporting Organization/Advisory Committee/Stakeholder Group/Constituency regarding the charter topics, as well as any positions or interests members wanted to share on behalf of their groups. To further support fulsome discussion, the leadership team regularly deployed informal polls in the meeting Zoom room to get a better sense of the "temperature of the room" and to prompt the sharing of perspectives and viewpoints that may not otherwise be voiced through less structured interaction.

For those working group members who were less comfortable speaking on calls, the leadership team encouraged additional feedback on the mailing list and through written contributions to working group documents.

Use of Working Documents

The working group used a series of working documents, organized per charter topic, to support its deliberations. Archives of the working documents are maintained on the working group [wiki](#). When a new charter topic was introduced, the leadership team provided a working document for the topic, including (i) charter questions related to that topic and for each charter question, (ii) context from the Transfer Policy Status Report, and (iii) relevant inputs received from community groups through early outreach. As the working group progressed through discussions, staff captured a summary of deliberations on the charter question and eventually populated the document with draft charter question responses and draft preliminary recommendations to support further discussion and refinement of the text.

Working documents were updated on an ongoing basis and working group members were encouraged to provide comments and input in the working documents between calls.

Diagrams

To further support deliberations and document the expected impact of proposed recommendations, the working group developed a swim lane diagram to visually represent the possible future-state process flow for inter-Registrar transfers as it will exist if all recommendations are approved and implemented. The diagrams serve as a working document to support the deliberations process and are not intended to be authoritative, but are included in this Initial Report to demonstrate the working group's understanding of the recommendations' impact on the inter-Registrar transfer and Change of Registrant Data processes. The diagrams are included in the last Annex of this report.

Data and Metrics

The [Transfer Policy Status Report](#) produced by ICANN org in 2019 served as the working group's primary resource for data and metrics related to inter-Registrar transfers. In the course of its deliberations, the working group identified additional data that would be valuable to support its work. The additional data provided by ICANN org's Contractual Compliance Department in response to these requests is available on the working group's [wiki](#).

ICANN org Interaction

To help support a smooth transition from policy development to eventual implementation of GNSO Council adopted and ICANN Board approved recommendations, the working group has been supported by early and ongoing engagement with ICANN org subject matter experts. Liaisons from ICANN org's Global Domains and Strategy (GDS) and Contractual Compliance departments regularly attended working group calls, providing input and responding to questions where it was possible to do so in real time. The liaisons acted as a conduit for working

group questions to ICANN org that required additional research or input. The liaisons also facilitated early review of working group draft outputs by ICANN org subject matter experts.

Accountability to the GNSO Council

As is now the case with all GNSO working groups, the working group delivered monthly “project packages” to the GNSO Council to update the Council on the status of its work. An archive of these packages is available on the [wiki](#). The GNSO Council Liaisons, Greg DiBiase and Osvaldo Nova, ³³ served as additional points of connection between the Council and the working group.

Conclusion and Next Steps

This Initial Report will be posted for public comment for 60 days. The working group will review the public comments received on this Initial Report and consider whether any changes need to be made to its Initial Report before submitting its Final Report to the GNSO Council.

³³ On 19 January 2023, the GNSO Council voted to approve Osvaldo Nova as the new GNSO Council Liaison to the TPR Working Group. Osvaldo Nova took over for Greg DiBiase who served as the Liaison beginning in April 2021.

Annex 6 – Working Group Membership and Attendance

The working group held its first meeting in April 2021. Recordings and transcripts of the group's discussions can be found on its [wiki space](#). It has conducted its work primarily through weekly conference calls, in addition to email exchanges on its mailing list.

As instructed by the GNSO Council, the working group prepared a [work plan](#), which it reviewed on a regular basis. The working group Chair and the GNSO Council Liaison to the working group also provided regular reports to the GNSO Council regarding the status and progress of the group's work. Details of the project schedule, attendance and action items can be found in the monthly project packages.

The working group email archives can be found [here](#).

Plenary Meetings:

- 150 Plenary calls (w/ 8 canceled) for 212.0 call hours for a total of 5930.5 person hours

Small Team Meetings:

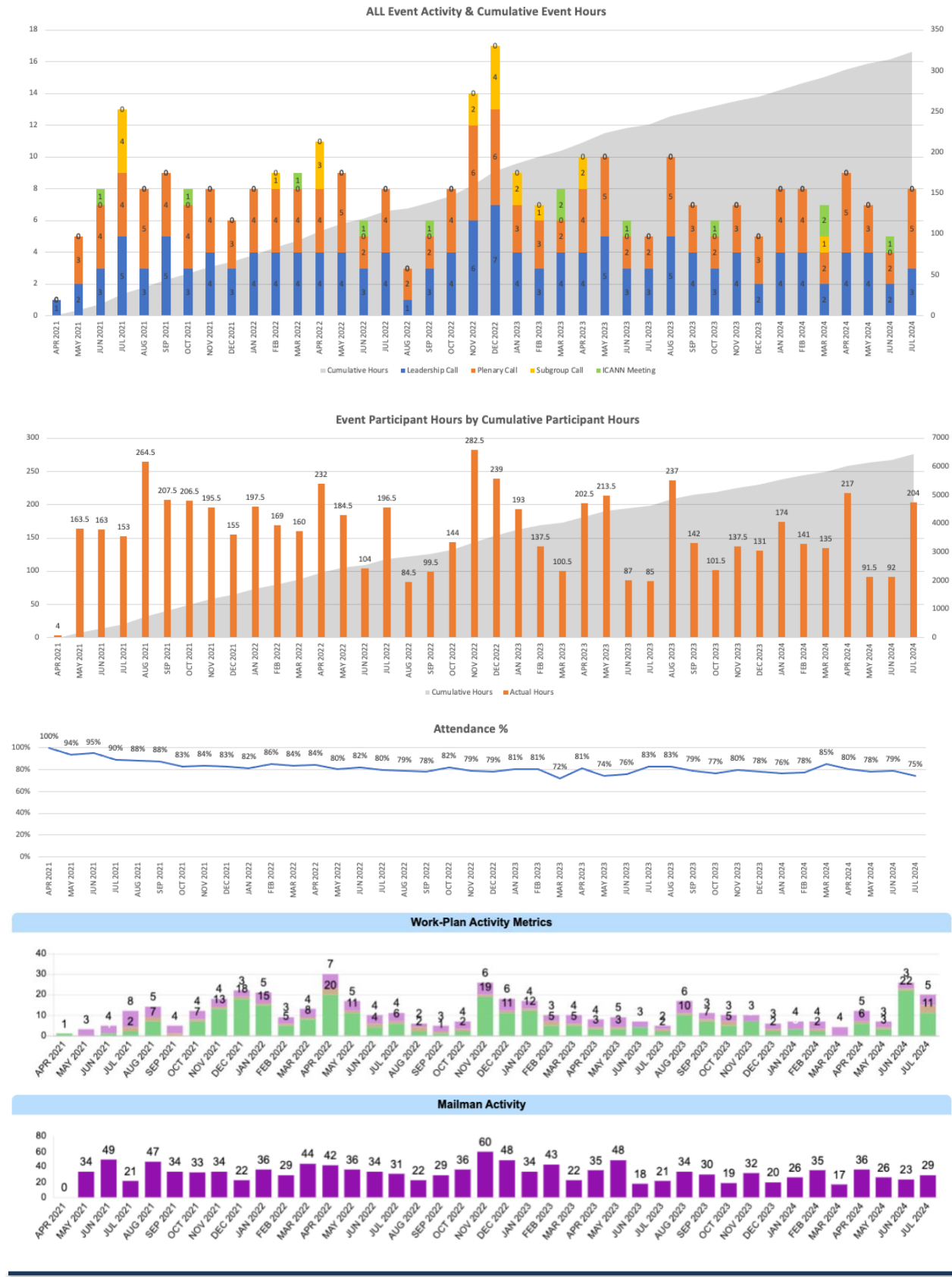
- 20 Small team calls for 20.0 call hours for a total of 176.0 person hours

Leadership Meetings:

- 144 Leadership calls (w/22 canceled) for 68.0 call hours for a total of 367.5 person hours

Total Attendance Rating: 74.8%

Working Group Activity Metrics:



The participants of the working group are:

	Invited	Attended	Percent	Role	SOI	Start Date	Depart Date
Member	3214	2304	71.7%				
ALAC	262	151	57.6%				
Nanghaka Daniel Khauka	131	41	31.3%		SOI	04.05.2021	
Steinar Grøtterød	131	110	84.0%		SOI	05.05.2021	
BC	136	120	88.2%				
Zak Muscovitch	136	120	88.2%		SOI	23.04.2021	
GNSO Council	509	394	77.4%				
Gregory DiBiase	120	61	50.8%	Liaison	SOI	04.06.2021	21.12.2022
Oswaldo Novoa	113	62	54.9%	Liaison	SOI	21.12.2022	
Roger Carney	276	271	98.2%	Chair	SOI	23.04.2021	
IPC	262	53	20.2%				
Mike Rodenbaugh	131	45	34.4%		SOI	21.04.2021	
Salvador Camacho Hernandez	131	8	6.1%		SOI	26.04.2021	
ISPCP	135	107	79.3%				
John Woodworth	135	107	79.3%		SOI	14.04.2021	
NCSG	135	84	62.2%				
Juan Manuel Rojas	62	40	64.5%		SOI	22.06.2022	
Kenneth Herman	39	37	94.9%		SOI	25.07.2023	
Raoul Plommer	34	7	20.6%		SOI	12.07.2022	27.06.2023
RrSG	1406	1195	85.0%				
Catherine Paletta	133	97	72.9%		SOI	27.04.2021	
Eric Rokobauer	130	118	90.8%		SOI	26.04.2021	
Jody Kolker	134	126	94.0%		SOI	07.05.2021	
Jothan Frakes	124	118	95.2%		SOI	23.04.2021	
Keiron Tobin	73	62	84.9%		SOI	07.06.2021	10.02.2023
Nan Chu	125	112	89.6%		SOI	06.05.2021	
Owen Smigelski	143	121	84.6%		SOI	27.04.2021	
Prudence Malinki	131	105	80.2%		SOI	27.04.2021	
Richard Merdinger	4	4	100.0%		SOI	05.05.2021	07.06.2021
Sarah Wyld	134	114	85.1%		SOI	23.04.2021	
Theo Geurts	131	117	89.3%		SOI	23.04.2021	
Thomas Keller	16	9	56.3%		SOI	26.04.2021	27.09.2021
Volker Greimann	128	92	71.9%		SOI	24.04.2021	
RySG	238	187	78.6%				
James Galvin	139	107	77.0%		SOI	27.04.2021	
Richard Wilhelm	99	80	80.8%		SOI	23.11.2022	
SSAC	131	13	9.9%				
Stephen Crocker	131	13	9.9%	SME	SOI	26.04.2021	

	Invited	Attended	Percent	Role	SOI	Start Date	Depart Date
Alternate	832	723	86.9%				
ALAC	93	82	88.2%				
Lutz Donnerhacke	47	43	91.5%		SOI	08.05.2021	
Raymond Selorm Mamattah	46	39	84.8%		SOI	04.05.2021	
BC	116	115	99.1%				
Arinola Akinyemi	116	115	99.1%		SOI	12.08.2021	
NCSG	158	72	45.6%				
Farzaneh Badiei	59	18	30.5%		SOI	24.07.2023	
Wisdom Donkor	99	54	54.5%		SOI	01.06.2021	
RrSG	439	428	97.5%				
Andrew Reberry	5	4	80.0%		SOI	23.04.2021	
Arnaud Wittersheim	97	96	99.0%		SOI	05.05.2021	
Benny Samuelson	25	25	100.0%		SOI	23.04.2021	
Christopher Patterson	39	39	100.0%		SOI	14.05.2021	
Essie Musailov	108	106	98.1%		SOI	23.04.2021	
Heidi Revels	19	19	100.0%		SOI	24.07.2023	
Jacques Blanc	7	4	57.1%		SOI	29.04.2021	
Jothan Frakes	13	13	100.0%		SOI	23.04.2021	
Min Feng	5	2	40.0%		SOI	26.04.2021	
Pam Little	2	1	50.0%		SOI	26.04.2021	30.05.2023
Richard Brown	119	119	100.0%		SOI	26.04.2021	
RySG	22	22	100.0%				
Carolyn Mitchell	22	22	100.0%		SOI	07.03.2023	
NPOC	4	4	100.0%				
Bolutife Adisa	4	4	100.0%		SOI	25.07.2023	
Grand Total	4046	3027	74.8%				

There is a total of 44 Observers to the working group.

ICANN org Policy Staff Support for the working group:

						Start Date	Depart Date
Staff - Assigned							
ICANN							
Berry Cobb						18.02.2021	
Caitlin Tubergen						18.02.2021	
Christian Wheeler						27.07.2023	
Devan Reed						16.11.2021	
Emily Barabas						18.02.2021	17.07.2023
Feodora Hamza						22.02.2024	
Holida Yanik				Liaison		30.04.2021	
Isabelle Colas				Liaison		10.06.2021	
Julia Bisland						18.02.2021	
Julie Hedlund						18.02.2021	
Terri Agnew						18.02.2021	
John Emery						14.05.2024	

Annex 7 – Community Input

Request for Input

According to the GNSO’s PDP Manual, a PDP working group should formally solicit statements from each GNSO Stakeholder Group and Constituency at an early stage of its deliberations. A PDP working group is also encouraged to seek the opinion of other ICANN Supporting Organizations and Advisory Committees who may have expertise, experience or an interest in the issue. As a result, the working group reached out to all ICANN Supporting Organizations and Advisory Committees as well as GNSO Stakeholder Groups and Constituencies with a request for input at the start of its deliberations. In response, statements were received from:

- The GNSO Business Constituency (BC)
- The Registries Stakeholder Group (RySG)
- The At-Large Advisory Committee (ALAC)
- The Security and Stability Advisory Committee (SSAC)

The full statements can be found on the working group wiki here:

<https://community.icann.org/x/tIT8CQ>.

Review of Input Received

All the statements received were added to the relevant working documents (organized by topic) and considered by the working group in the context of deliberations on each topic.

Annex 8 – EPDP Phase 1, Rec. 27, Wave 1 Analysis

For context on this analysis, please see pages 52-56 of the [Final Issue Report](#).

Wave 1 Analysis Key Points	TPR Working Group Response
<p>1. Transfer Policy section I.A.1.1 provides that either the Registrant or <i>the Administrative Contact</i> can approve or deny a transfer request. (emphasis added) 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.</p>	<p>In its current set of recommendations, the TPR working group does not include the Administrative Contact as an entity that can approve an inter-Registrar transfer; instead, the recommendations only refer to the Registered Name Holder, or, in some instances, the “Registered Name Holder or their designated representative.”</p> <p>In light of the obsolescence of the Administrative Contact under the EPDP Phase 1 recommendations, any reference to an “Administrative Contact” or “Transfer Contact” within the Transfer Policy MUST be eliminated and replaced with “Registered Name Holder” unless specifically indicated, per Recommendation 2. For example, Recommendation 5, et. al., refers to the “Registered Name Holder or their designated representative”.</p>
<p>2. Transfer Policy 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.</p>	<p>As noted above in Key Point 1, the recommendations currently refer to the “Registered Name Holder” instead of the “Transfer Contact”, noting that the Registered Name Holder is the now the valid transfer authority, rather than the “Transfer Contact” or “Administrative Contact”.</p>
<p>3. Transfer Policy section I.A.3 enumerates the reasons a registrar of record may deny a transfer. These include section 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</p>	<p>The working group is recommending that the reference to Administrative Contact in Section I.A.3.7.2 must be removed due to the EPDP recommendation for elimination of the Administrative Contact. See also TPR Recommendation 2.</p>

<p>Contact data is no longer collected by the registrar. Section I.A.3 also enumerates the reasons a registrar of record may not use to deny a transfer request. These include section 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.</p>	
<p>4. Transfer Policy 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.</p>	<p>The WG did not express an objection to the Wave 1 assertion that paragraph I.A.4.6.5 is likely not affected by the new Registration Data Policy. The WG did note that, in the event the WG proposes to further detail the requirements of TEAC processing and retention requirements (for example, by recommending these communications occur solely within the Naming Services Portal or its successor), the WG may need to revisit this item to ensure there is no conflict.</p> <p>The working group’s recommendations did not require revisiting its initial assertion that there is no conflict.</p>
<p>5. Transfer Policy 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.</p>	<p>In its recommendations, the working group is recommending eliminating the requirement that the Gaining Registrar send a Gaining Form of Authorization.</p> <p>For further rationale on the proposed elimination of the Gaining FOA, please see the working group’s response to charter question a1.</p> <p>With respect to the Losing FOA, the working group is recommending retaining the Losing FOA requirements with minor modifications, although the working group is recommending that the term “Transfer Confirmation” is used in place of the term Losing FOA. For further information, please see Recommendation 17.</p>
<p>6. Transfer Policy 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</p>	<p>The working group has updated the definition of Change of Registrant Data in Recommendation 25.</p>

<p>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.</p>	<p>Rec 25: The working group recommends that the Transfer Policy and all related policies MUST use the term “Change of Registrant Data” in place of the currently-used term “Change of Registrant”. This recommendation is for an update to terminology only and does not imply any other changes to the substance of the policies.</p> <p>Rec 25.3 provides that additions and/removals of P/P service Provider data do not amount to a Change of Registrant Data (CORD), so not all changes to the public RDDS will amount to a CORD.</p> <p>The working group also recommends eliminating Section II.B “Availability of Change of Registrant” in Recommendation 26 as it is unnecessary and redundant of existing policies.</p>
<p>7. Transfer Policy 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.</p>	<p>In recommendation 25.1, the working group recommends changing the definition of Change of Registrant to Change of Registrant Data, and the Administrative Contact field is no longer included in this definition.</p>
<p>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</p>	<p>For terminology consistency, the working group is recommending replacing current references to Whois to RDDS throughout the Transfer Policy, including in the updated standalone Change of Registrant Data policy, for any references to Whois that remain. (Please see response to Key Item 9 below for more detail and Recommendation 1.)</p>

<p>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.</p>	
<p>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:</p> <p>(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:</p> <p>(a1) The Gaining Registrar is not REQUIRED to obtain a Form of Authorization from the Transfer Contact.</p> <p>(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.</p> <p>(b) As used in the Transfer Policy:</p> <p>(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".</p> <p>(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".</p>	<p>In its recommendations, the working group is recommending eliminating the requirement that the Gaining Registrar send a Gaining Form of Authorization (Recommendation 15).</p> <p>In Recommendation 1, the working group is recommending the terminology changes from EPDP Phase 1, Recommendation #24. Specifically:</p> <p>(b) As used in the Transfer Policy:</p> <p>(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".</p> <p>(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".</p> <p>(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".</p> <p>(b4) The term "Whois" SHALL have the same meaning as "RDDS".</p> <p>With respect to (c) and (d), the working group has a list of very specific recommendations regarding generating and updating the TAC (formerly referred to as Auth-Info Code) that can be found in Section 3.2 of the Initial Report.</p>

<p>(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".</p> <p>(b4) The term "Whois" SHALL have the same meaning as "RDDS".</p> <p>(c) Registrar and Registry Operator SHALL follow best practices in generating and updating the "AuthInfo" code to facilitate a secure transfer process.</p> <p>(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.</p> <p>These requirements are being implemented as part of implementing the Registration Data Policy.</p>	
<p>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.</p>	<p>The working group has methodically worked through its charter questions, which has enabled it to review previously identified and longstanding issues in the Transfer Policy by proposing slight adjustments to specific transfer issues and/or proposing new methods.</p>
<p><i>Cross-reference: Transfer Policy 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.</i></p>	<p>In Recommendation 1, the working group is recommending the terminology changes from EPDP Phase 1, Recommendation #24. Specifically:</p> <p>(b) As used in the Transfer Policy:</p> <p>(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".</p> <p>(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".</p> <p>(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".</p>

	<p>(b4) The term "Whois" SHALL have the same meaning as "RDDS".</p> <p>The terminology updates shall also apply to the new standalone Change of Registrant Data Policy.</p>
<p><i>Cross-reference: Transfer Policy 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.</i></p>	<p>In Recommendation 1, the working group is recommending the terminology changes from EPDP Phase 1, Recommendation #24. Specifically:</p> <p>(b) As used in the Transfer Policy:</p> <p>(b1) The term "Whois data" SHALL have the same meaning as "Registration Data".</p> <p>(b2) The term "Whois details" SHALL have the same meaning as "Registration Data".</p> <p>(b3) The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".</p> <p>(b4) The term "Whois" SHALL have the same meaning as "RDDS".</p> <p>The terminology updates shall also apply to the new standalone Change of Registrant Data Policy.</p>
<p>Transfer Dispute Resolution Policy</p>	
<p>1. TDRP 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.</p>	<p>The working group agrees with the assertion that TDRP Section 2.2 can be maintained under the Registration Data Policy.</p>

<p>2. TDRP 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.</p>	<p>The working group recognizes that the above-cited provisions of the TDRP specify TDRP complainant information that may include personal data. The working group notes that the implementation of EPDP Recommendations 22 and 26, which recommend data protection agreements/arrangements between ICANN org and dispute resolution providers and data escrow providers, respectively, is currently ongoing. In the event the working group provides additional recommendations that require the processing of personal data that is not registration data, the WG notes that the appropriate parties, such as those implementing the EPDP recommendations, should be duly informed.</p>
<p>TDRP 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.</p>	<p>The working group noted that references to Whois data do indeed need to be updated.</p> <p>The working group made the following recommendation in its Initial Report:</p> <p>Recommendation 1: The working group recommends the following specific terminology updates to the Transfer Policy:</p> <p>The term "Whois data" SHALL have the same meaning as "Registration Data".</p> <p>The term "Whois details" SHALL have the same meaning as "Registration Data".</p> <p>The term "Publicly accessible Whois" SHALL have the same meaning as "RDDS".</p> <p>The term "Whois" SHALL have the same meaning as "RDDS". For the avoidance of doubt, the terms referenced in above in Recommendation 1 (i) - (iv) are intended to correspond to the definitions in the Registrar Accreditation Agreement ("RAA"). In the event of any inconsistency, the RAA definitions, if updated, will supersede. The working group also recommends that the</p>

	<p>outdated terms should be replaced with the updated terms, e.g., all references to “Whois Data” should be replaced with the term “Registration Data,” etc.</p> <p>The WG notes similar updates will need to be made to the TDRP.</p>
<p>TDRP 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.</p>	<p>The working group noted that this provision may implicate public, redacted, and/or privacy/proxy customer data. The working group also noted that relevant Whois modifications may include nameserver data, not just registrant contact data. Proposed updates have been made to the draft TDRP in Annex 9.</p>
<p>TDRP 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.</p> <p>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.</p>	<p>Some members of the WG noted that TDRP section 3.2.4 could be stated at a higher level to ask the Panel to review the documentation provided to determine whether a violation of the Transfer Policy has occurred. Support Staff has proposed updated language on what this could look like.</p> <p>Other WG members noted that the Panel should request the redacted registration data from the Gaining Registrar, similar to how this is done in a UDRP proceeding. Support Staff has also proposed language so that the WG could see how this could look.</p> <p>Outstanding: need to decide</p>

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.

Annex 9 – Draft Edits to Transfer Dispute Resolution Policy (EPDP Rec. 27)

Registrar Transfer Dispute Resolution Policy

NOTE: On 26 January 2020, 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 a Standardized Form of Authorization (FOA). ICANN Contractual Compliance has deferred and will continue to defer enforcement of Section I(A)(2.1) of the Transfer Policy until the matter is settled in the GNSO Council's Transfer Policy Review, which is currently ongoing. Accordingly, the absence of a Standardized Form of Authorization (FOA) from the Gaining Registrar shall not result in a decision of transfer reversal under Section 3.2.4(ii) 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 following procedures apply. It is very important for Registrars to familiarize themselves with the Transfer Dispute Resolution Policy (TDRP) as described in this document before filing a dispute. Transfer dispute resolution fees can be substantial. It is critical that Registrars fully understand the fees that must be paid, which party is responsible for paying those fees and when and how those fees must be paid.

This version of the TDRP and corresponding procedures will apply to all Complaints filed on or after 1 December 2016.

1. Definitions

1.1 Complainant

A party bringing a Complaint under the TDRP. A 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) under this Policy.

1.2 Complaint

The initial document in a TDRP proceeding that provides the allegations and claims brought by the Complainant against the Respondent.

1.3 Dispute Resolution Panel

The Dispute Resolution Panel shall mean an administrative panel appointed by a Dispute Resolution Provider ("Provider") to decide a Complaint concerning a dispute under the TDRP.

1.4 Dispute Resolution Provider

The Dispute Resolution Provider must be an independent and neutral third party that is neither associated nor affiliated with the Respondent, Complainant, or the Registry Operator under which the disputed domain name is registered. ICANN shall have the authority to accredit one or more independent and neutral Dispute Resolution Providers according to criteria developed in accordance with the TDRP.

1.5 Form of Authorization (FOA)

The standardized form of consent that the Gaining Registrar and Losing Registrar are required to use to obtain authorization from the Registrant or Administrative Contact in order to properly process the transfer of domain name sponsorship from one Registrar to another.

1.6 Gaining Registrar

The registrar who seeks to become the Registrar of Record by submitting a transfer request.

1.7 Invalid Transfer

A transfer that is found non-compliant with the Transfer Policy.

1.8 Losing Registrar

The registrar who was the Registrar of Record at the time a request for the transfer of domain is submitted.

1.9 NACK

A denial of a request for transfer by the Losing Registrar.

1.10 Registrant

The individual, organization, or entity that holds the right to use a specific domain name for a specified period of time.

1.11 Registrar of Record

The Registrar who sponsors a domain name at the Registry.

1.12 Registry (Registry Operator)

The organization authorized by ICANN to provide registration services for a given TLD to ICANN-accredited Registrars.

1.13 Respondent

A party against whom a Complaint is brought. Under the TDRP, the Respondent can be a Losing Registrar in the case of an improper (NACK), a Gaining Registrar in the case of an alleged fraudulent transfer, or the Registrar of Record.

1.14 Supplemental Rules

The Supplemental Rules shall mean those rules adopted by the Provider administering a proceeding to supplement the TDRP. Supplemental Rules shall be consistent with the TDRP and shall cover topics such as fees, word and page limits and guidelines, the means for communicating with the Provider, and the form of cover sheets.

1.15 Transfer Policy

The ICANN Consensus Policy governing the transfer of sponsorship of registrations between registrars as referenced in the Registry-Registrar Agreement executed between a Registrar and the Registry, as well as the Registrar Accreditation Agreement which is executed between ICANN and all ICANN-accredited Registrars.

2. Dispute Resolution Process

2.1 Filing a Complaint

The Complainant may file a Complaint with a Dispute Resolution Provider. The decision of the Dispute Resolution Panel is final, except as it may be appealed to a court of competent jurisdiction in accordance with Section 3.4 of the TDRP.

2.2 Statute of Limitations

A dispute must be filed no later than twelve (12) months after the alleged violation of the Transfer Policy. In the case where a Losing Registrar alleges that a transfer was in violation of the Transfer Policy, the date the transfer was completed shall be deemed the date on which the "alleged violation" took place. In the case where a Gaining Registrar alleges that a transfer should have taken place, the date on which the NACK (as defined below) was received by the Registry, shall be deemed the date on which the "alleged violation" took place.

3. Dispute Procedures

3.1 Registrar files a Request for Enforcement with a Dispute Resolution Provider

3.1.1 Either the Gaining Registrar or Losing Registrar may submit a Complaint. This must be done in accordance with the Supplemental Rules adopted by the applicable Dispute Resolution Provider.

3.1.2 The Complaint shall be submitted to the Dispute Resolution Provider and to the Respondent in electronic form and shall:

- i. Request that the Complaint be submitted for decision in accordance with the TDRP and the applicable Supplemental Rules;
 - ii. Provide the name, postal and e-mail addresses, and the telephone and fax numbers of the Complainant and those representatives authorized by the Complainant to act on behalf of the Complainant in the administrative proceeding;
 - iii. Provide the name of the Respondent and all information (including any postal and e-mail addresses and telephone and fax numbers) known to Complainant regarding how to contact Respondent or any representative of Respondent, including contact information based on pre-complaint dealings;
 - iv. Specify the domain name(s) that is/are the subject of the Complaint;
 - v. Specify the incident(s) that gave rise to the dispute;
-

- vi. Describe, in accordance with the Transfer Policy, the grounds on which the Complaint is based;
- vii. State the specific remedy being sought (either approval or denial of the transfer);
- viii. Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the Complaint;
- ix. Certify that a copy of the Complaint, together with the cover sheet as prescribed by the Provider's Supplemental Rules, has been sent or transmitted to the Respondent; and
- x. Conclude with the following statement followed by the signature of the Complainant or its authorized representative:

"<insert name of Complainant> agrees that its claims and remedies concerning the registration of the domain name, the dispute, or the dispute's resolution shall be solely against the Respondent and waives all such claims and remedies against the Dispute Resolution Provider as well as its directors, officers, employees, and agents, except in the case of deliberate wrongdoing or gross negligence."

"<insert name of Complainant> certifies that the information contained in this Complaint is to the best of Complainant's knowledge complete and accurate, that this Complaint is not being presented for any improper purpose, such as to harass, and that the assertions in this Complaint are warranted under the TDRP and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."

3.1.3 The Complaint may relate to more than one domain name, provided that the domain names involve the same Complainant and Respondent and that the claims arise out of the same or similar factual circumstances.

3.1.4 The Complaint shall annex the following documentary evidence (as applicable and available) in electronic form if possible, together with a schedule indexing such evidence:

- i. For the Gaining Registrar:
 - a. **Completed Form of Authorization ("FOA")**
-

-
- b. ~~Copy of the Whois RDDS output for the date transfer was initiated, which was used to identify the authorized Transfer Contacts~~
 - c. ~~Copy of evidence of identity used~~
 - d. Copy of a bilateral agreement, final determination of a dispute resolution body or court order in cases when the Registrant of Record is being changed simultaneously with a Registrar Transfer ~~(where applicable)~~
 - e. Copies of all communications made to the Losing Registrar with regard to the applicable transfer request along with any responses from the Losing Registrar
 - ii. For the Losing Registrar:
 - a. Completed FOA from the Losing Registrar
 - b. Copy of the ~~Whois RDDS~~ output for the date the transfer was initiated
 - c. Relevant history of ~~Whois~~ ~~Registration Data~~³⁴ modifications made to the applicable registration
 - d. Evidence of one of the following if a transfer was denied:
 - § fraud;
 - § Pending UDRP proceeding that the Registrar has been informed of;
 - § URS proceeding or URS Suspension that the Registrar has been informed of;
 - § Pending dispute under the Transfer Dispute Resolution Policy;
 - § court order by a court of competent jurisdiction;
 - § Registrant or administrative contact identity dispute in accordance with Section 4 of the Transfer Policy [Registrar of Record Requirements]
 - § applicable payment dispute along with evidence that the registration was put on HOLD status;
 - § express written objection from the Registered Name Holder or Administrative Contact;

³⁴ For clarity, relevant Registration Data modifications may include relevant modifications to: (i) public RDDS, (ii) redacted Registration Data, and/or (iii) Privacy/Proxy Customer data from an Affiliated Privacy or Proxy Service Provider.

§ LOCK status along with proof of a reasonable means for the registrant to remove LOCK status as per Section __ of Exhibit __ to this Agreement;

~~§ 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.~~

§ domain name within 30 days of initial registration; or

§ domain name within 30 days of a prior transfer.

- e. Copies of all communications made to the Gaining Registrar with regard to the applicable transfer request along with any responses from the Gaining Registrar.

[[DRAFT ADDED STEP: The Provider shall submit a verification request to the sponsoring Registrar. The verification request will include a request to Lock the domain name.]]

[[DRAFT ADDED STEP: Within two (2) business days of receiving the Provider's verification request, the sponsoring Registrar shall provide the information requested in the verification request and confirm that a Lock of the domain name has been applied. The Lock shall remain in place through the remaining Pendency of the TDRP proceeding.]]

3.2 The Respondent shall have seven (7) calendar days from receipt of the Complaint to prepare a Response to the Complaint ("Response").

3.2.1 The Response shall be submitted in electronic form to both the Dispute Resolution Provider and Complainant and shall:

- i. Respond specifically to the statements and allegations contained in the Complaint (This portion of the response shall comply with any word or page limit set forth in the Dispute Resolution Provider's Supplemental Rules.);
- ii. Provide the name, postal and e-mail addresses, and the telephone and fax numbers of the Respondent (non-filing Registrar);
- iii. Identify any other legal proceedings that have been commenced or terminated in connection with or relating to any of the domain name(s) that are the subject of the Complaint;
- iv. State that a copy of the Response has been sent or transmitted to the Complainant;

- v. Conclude with the following statement followed by the signature of the Respondent or its authorized representative:

"Respondent certifies that the information contained in this Response is to the best of Respondent's knowledge complete and accurate, that this Response is not being presented for any improper purpose, such as to harass, and that the assertions in this Response are warranted under these Rules and under applicable law, as it now exists or as it may be extended by a good-faith and reasonable argument."; and

- vi. Annex any documentary or other evidence upon which the Respondent relies, together with a schedule indexing such documents.

3.2.2 At the request of the Respondent, the Dispute Resolution Provider may, in exceptional cases, extend the period of time for the filing of the response, but in no case may the extension be more than an additional five (5) calendar days. The period may also be extended by written stipulation between the Parties, provided the stipulation is approved by the Dispute Resolution Provider.

3.2.3 If a Respondent does not submit a response, in the absence of exceptional circumstances, the Dispute Resolution Panel appointed by the Dispute Resolution Provider shall decide the dispute based upon the Complaint.

3.2.4 The Dispute Resolution Panel appointed by the Dispute Resolution Provider must review all applicable documentation and, where applicable, compare registrant/contact data with that contained within the RDDS authoritative Whois database. Following its review of all applicable documentation, the Dispute Resolution Panel ~~and~~ must determine whether a violation of the Transfer Policy occurred reach a conclusion not later than thirty (30) days after receipt of Response from the Respondent.

- i. If the Dispute Resolution Panel is unable to determine whether a violation of the Transfer Policy occurred using the documentation provided, the registrant/contact data does not match the data listed in authoritative Whois RDDS, the Dispute Resolution Panel MAY ~~should~~ contact each Registrar and require additional documentation.

- ii. ~~If the Gaining Registrar is unable to provide a complete FOA with data matching that contained within the authoritative Whois database RDDS at the time of the transfer request, then the Dispute Resolution Panel shall find that the transfer should be reversed. In the case of a thick Registry, if the Registrar of Record's Whois RDDS is not~~

accessible or invalid, the applicable Registry Operator's Whois RDDS should be used. In the case of a thin Registry, if the Registrar of Record's Whois RDDS is not accessible or is invalid, the Dispute Resolution Provider may place the dispute on hold until such time as the problem is resolved.

iii. In the case where a Losing Registrar NACKs a transfer, the Losing Registrar must provide evidence of one of the factors for which it is allowed to NACK as set forth in Section 3.1.4(ii)(d) of the TDRP. If the Losing Registrar cannot provide evidence that demonstrates any of the factors, and the Gaining Registrar is able to demonstrate compliance with the Transfer Policy, provides to the Dispute Resolution Provider a complete FOA with data matching that contained within the authoritative Whois database RDDS at the time of the transfer request, then the transfer should be approved.

iv. 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.

v. Resolution options for the Dispute Resolution Panel are limited to the following:

- a. Approve Transfer
- b. Deny the Transfer (This could include ordering the domain name be returned to the Losing Registrar in cases where a Transfer has already occurred.)

vi. Transfers from a Gaining Registrar to a third registrar, and all other subsequent transfers, are invalid if the Gaining Registrar acquired sponsorship of the domain name(s) at issue through an Invalid Transfer, as determined through the dispute resolution process set forth in this Transfer Dispute Resolution Policy.

vii. In the event the Dispute Resolution Panel determines that an Invalid Transfer occurred, the domain shall be transferred back to the registrar that was Registrar of Record immediately prior to the Invalid Transfer.

3.3 Fees for Dispute Resolution Service

3.3.1 The applicable Dispute Resolution Provider shall determine the applicable filing fee ("Filing Fees"). The specific fees along with the terms and conditions governing the actual payment of such fees shall be included in the Dispute Resolution Provider's Supplemental Rules.

3.3.2 In the event that the Complainant does not prevail in a dispute, the Filing Fees shall be retained by the Dispute Resolution Provider.

3.3.3 In the event that the Complainant prevails in a dispute, the Respondent, must submit to the Dispute Resolution Provider, the Filing Fees within fourteen (14) calendar days after such decision. In such an event, the Dispute Resolution Provider shall refund to the Complainant, whichever applicable, the Filing Fees, no later than fourteen (14) calendar days after it receives the Filing Fees from the Respondent. Such fees must be paid regardless of whether a court proceeding is commenced in accordance with Section 3.4 below. Failure to pay Filing Fees to the Dispute Resolution Provider may result in the loss of accreditation by ICANN.

3.4 Availability of Court Proceedings

The procedures set forth above shall not prevent a Registrar from submitting a dispute to a court of competent jurisdiction for independent resolution before such administrative proceeding is commenced or after such proceeding is concluded. If a Dispute Resolution Panel decides a domain name registration should be transferred (either to the Gaining Registrar, or alternatively, back from the Gaining Registrar to the Losing Registrar), such Registrar will wait fourteen (14) calendar days after it is informed of the decision before implementing that decision. The Registry will then implement the decision unless it has received from either of the parties to the dispute during that fourteen (14) calendar day period official documentation (such as a copy of a complaint, file-stamped by the clerk of the court) that a lawsuit has commenced with respect to the impacted domain name(s). If such documentation is received by the Registry, as applicable, within the fourteen (14) calendar day period, the decision will not be implemented until (i) evidence is presented that the parties have resolved such dispute; (ii) evidence is presented that the lawsuit has been dismissed or withdrawn; or (iii) a copy of an order from such court dismissing the lawsuit or ordering certain actions with respect to the domain name.

3.5 Decision Publication

3.5.1. The relevant Dispute Resolution Provider shall publish any decision made with respect to a transfer dispute initiated under the TDRP. All decisions under this Policy will be published in full over the Internet except when the Panel, convened by the Dispute Resolution Provider, in

an exceptional case, determines to redact portions of its decision. In any event, the portion of any decision determining a complaint to have been brought in bad faith shall be published.

3.5.2. Decision reports shall include, at a minimum:

- i. The domain name under dispute;
- ii. The names of parties involved in the dispute;
- iii. The full decision of the case;
- iv. The date of the implementation of the decision.

3.5.3 If the Dispute Resolution Provider believes a decision should not be published, the Dispute Resolution Provider should confer with ICANN and publish the decision if so directed.

3.5.4. Publication does not apply to TDRP Complaints filed prior to 1 December 2016.

Annex 10 – Draft edits to Section I.B.1 of the Transfer Policy (Bulk Transfers)

Proposed edit to Section I.B.1

Current language: I.B.1 Transfer of the sponsorship of all the registrations sponsored by one Registrar as the result of

(i) a Registrar 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:

Potential Update for consideration: There are some instances that fall outside of the requirements in Section I(A) of the Transfer Policy. Specifically, ICANN org may authorize the transfer of a registrar's domain names through an ICANN-approved bulk transfer without the prior approval of the Registered Name Holder in the following instances:

(i) the Registrar or its assets are acquired by another ICANN-accredited Registrar;

(ii) the Registrar is no longer accredited with ICANN org;

(iii) the Registrar is no longer accredited with a Registry Operator(s) in a TLD(s), e.g., termination of Registry-Registrar Agreement(s)*

2. Additional instances that fall outside of the requirements in Section I(A) of the Transfer Policy include partial bulk transfers pre-authorized by ICANN org and offered by some Registry Operators. Specifically, a Registry Operator MAY permit a consenting Registrar to transfer a portion but not all of its domain names to another consenting Registrar in the following instances:

(i) one ICANN-accredited Registrar purchases, by means of a stock or asset purchase, merger or similar transaction, a portion but not all, of another ICANN-accredited Registrar's domain name portfolio in the TLD,

(ii) a newly-accredited Registrar (Gaining Registrar) requests a transfer of all domain names from the losing Registrar for which the gaining Registrar has served as the Reseller, or

(iii) -an agent of the Registrar, such as a Reseller or service provider, elects to transfer its portfolio of domain names to a new gaining registrar, and the registration agreement explicitly permits the transfer

Annex 11 – Additional Topics Discussed

Transfer Fees

In the course of discussing the topic of Denying (NACKing) Transfers, the working group considered whether it is appropriate to make a recommendation with respect to transfer fees, a topic that NCSG representatives raised in working group deliberations, and also a subject that was raised in public comments on the Phase 1(a) Initial Report. The working group noted that some Registrars charge the RNH a fee for transferring a domain away to another Registrar. The Transfer Policy does not prohibit such fees.

From one perspective, transfer fees can be burdensome, particularly for non-commercial applicants, and should be prohibited or limited. From another perspective, there are scenarios where such fees correspond to value-added services from the Registrar, and therefore the fees are appropriate. Further from this perspective, regulating fees charged by Registrars is typically outside the scope of GNSO policy development.

The working group recalled that the Transfer Policy does not contain any provisions allowing the Registrar to deny a transfer for non-payment of transfer fees, and therefore in practice, these fees are not a barrier to transfer. The working group also noted that in Recommendations 21 and 24, the working group has recommended clarifications to language specifying when a Registrar may and must not deny a transfer in relation to non-payment of registration fees.

Ultimately, the working group did not come to agreement to make recommendations on this topic, noting that it is important for Registrants to carefully review the registration agreement, which discloses any fees associated with transferring the domain to a new Registrar.

Sanctions

In working group deliberations and in public comment, the NCSG raised concerns that ordinary non-commercial registrants who are based in sanctioned countries or serving customers in sanctioned countries are sometimes prevented from transferring domains to a new Registrar, even in cases where the Registrar is not legally obligated to prevent the transfer under applicable law. In other cases, the RNH is given an insufficient notice period to find a new Registrar before the registration agreement is terminated. The NCSG requested that the working group consider whether these issues are in scope of the PDP.

The working group discussed the fact that Registrars are obligated to comply with national law and that it is up to each Registrar to determine how to do so. The working group considered that the issue of sanctions impacts many elements of the domain name lifecycle, including domain creation, renewal, suspension, and termination. To address this topic in isolation in the context of transfers could result in a fragmented approach to the issues presented. To the extent that the concerns are addressed through policy development, the working group believes that they should be addressed holistically.

The working group further noted that WS2 implementation is ongoing, which includes work related to specific concerns around sanctions. In particular, WS2 recommendation 4.1.3 recommends that ICANN clarify to Registrars “that the mere existence of their RAA with ICANN does not cause them to be required to comply with OFAC sanctions. ICANN should also explore various tools to remind registrars to understand the applicable laws under which they operate and to accurately reflect those laws in their customer relationships.”³⁵ The working group understands that the implementation of this recommendation may reduce the risk of Registrar over-compliance.

Additional Topic Suggested by SSAC

In its [submission providing early input](#) to the PDP, the SSAC recommended that the working group address the issue of ensuring DNSSEC operational continuity in the transfer of DNS service:

When a registrant bundles their DNS service with their registration, then it is essential that the transfer of DNS service be coordinated between the DNS service providers (who are most often the registrar when services are bundled) in order to ensure there is no discontinuity in DNS resolution (i.e., the registrant does not lose the ability to use their domain name).

When the domain name is DNSSEC-signed in the bundled scenario, there is an additional risk of failure to validate if the transfer is not properly coordinated. Best practice security principles would ordinarily treat a security failure more harshly than a non-existent domain, the consequences of which will vary by application.

These risks are substantially reduced during a registration transfer if a registrant uses a third party DNS service provider, one who is independent of the registration

³⁵ <https://www.icann.org/en/system/files/files/ccwg-acct-ws2-final-24jun18-en.pdf>

service provider. It is important to note that these risks are not specific to registration transfers; they are present whenever there is a change in DNS service providers.

The SSAC recommends the Transfer Policy Review Team consider these concerns and seek the necessary enhancements to the current process that will ensure a secure, stable, and resilient transfer solution in the best interest of the registrant.

The working group noted that this topic was not included in the Final Issue Report or the working group charter. While the working group acknowledges that it is an important subject area for additional work, the working group agreed that it is outside the scope of this PDP and is better addressed in another forum.

Annex 12 – Group 1A Swimlane

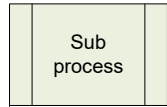
This page is intentionally left blank.

The next page will display the swimlane legend and the following page will be a PDF version of the swimlane appended to this report. Please refer to this [link](#) for a more consumable version of the swimlane where the PDF can be downloaded from the wiki.

Process Legend



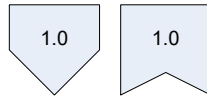
Process Step



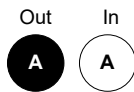
Sub-Process Step



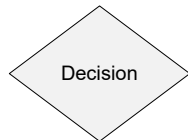
Process Input



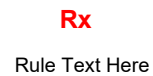
Off Page Reference



On Page Reference



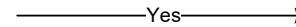
Decision



Process Rule



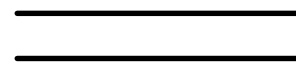
Begin of Process



Process Flow



Diversion to External Process



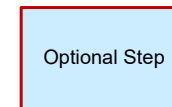
Parallel Process



Terminator of Process



External Process not Active



Optional Decision/Process Step

Transfer Policy (Inter-Registrar) – Proposed

