

# Initial Report on the Transfer Policy Review

**Category:** Policy

**Requester:** Generic Names Supporting Organization (GNSO)

**ICANN org Contact(s)** [policy-staff@icann.org](mailto:policy-staff@icann.org)

First Name

George

Last Name

Kirikos

Check if you prefer to have your affiliation displayed as the author of this submission, rather than the first and last name

Affiliation

Leap of Faith Financial Services Inc.

Email

george@loffs.com

## Instructions

This Public Comment forum seeks community feedback on the Initial Report published by the Transfer Policy Review (TPR) Policy Development Process (PDP) Working Group.

This is a new format for collecting public comments. It seeks to:

- Clearly link comments to specific sections of the Initial Report
- Encourage commenters to provide reasoning or rationale for their opinions
- Enable the sorting of comments so that the TPR PDP Working Group can more easily read all comments on each topic

There is no obligation to complete all sections within this form – respond to as many or as few questions as desired. Additionally, you can provide comments on the general content of the Initial Report or on new issues not raised by the Initial Report. To preview all questions in this form in Word format, you may refer to a [Word doc version here](#).

It is important that your comments include rationale. This is not a vote. The TPR PDP Working Group is interested in your reasoning so that the conclusions reached can be tested against the

reasoning of others. (This is much more helpful than comments that simply “agree” or “disagree”).

**NOTE:**

- Please refer to the specific recommendation and relevant section, page number, and/or Annex of the Initial Report for additional details and context about each recommendation.
- Your comments should take into account the scope of the PDP as described by the [Charter](#) and General Data Protection Regulation compliance.
- If you encounter difficulties submitting your Public Comment, please send an email to [policy-staff@icann.org](mailto:policy-staff@icann.org) and the TPR PDP Support Staff will assist you.
- The final date of this Public Comment proceeding is 23:59 UTC on 30 September 2024. Any comments received after that date will not be reviewed and discussed by the TPR PDP Working Group.

## Questions

### **Part A: TPR PDP Initial Report - Group 1(a)** **Recommendations #1-24**

#### **Recommendation #1: Terminology Updates: WHOIS**

Page 9 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #1:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #1, please indicate the revised wording and rationale here.

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

Page 10 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #2:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #2, please indicate the revised wording and rationale here.

## **Recommendation #3: Transfer Restriction After Initial Registration**

Page 10 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #3:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #3, please indicate the

revised wording and rationale here.

As stated on page 4, “only the policy recommendation text itself is meant to be considered authoritative.” Therefore, it is critical to note that the two footnotes are not actually incorporated into the recommendation text. To avoid any confusion, this recommendation should be rewritten as follows: (a) Replace the term “initial registration date” with “creation date”, and (b) Fully incorporate the content of footnote 2 into the main body of the recommendation itself. Without these changes, the recommendation fails to fully address the concern and does not effectively avoid doubt. Additionally, the use of “30 calendar days / 720 hours” creates unnecessary ambiguity. One registry or registrar might interpret “30 calendar days,” while another could use “720 hours,” and these are not always equivalent (due to differences in time, such as rounding, where 1:00 a.m. to 11:00 p.m. on the next day could be considered one calendar day but amounts to 46 hours). To avoid such inconsistencies, it is essential that the policy text specify 720 hours as the authoritative duration. The reference to “30 days” should only appear in the explanatory text, which is not authoritative. This approach should be applied consistently throughout the document to ensure clarity and uniform application. Please apply this logic universally, as I prefer not to repeat this comment for each instance where ambiguity arises.

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

Page 12 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #3:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #3, please indicate the revised wording and rationale here.

I would like to take this opportunity to further advocate for the adoption of a push-based transfer system, as fully documented in my company's prior submission: <https://freespeech.com/wp-content/uploads/2022/08/LEAP-comments-Transfers-Phase1a-20220814-FINAL.pdf> which I believe would offer a more comprehensive and permanent solution to transfer-related security issues. While the improvements to the TAC system reduce some risk, the fact remains that any shared-secret mechanism like TAC still presents vulnerabilities, particularly in cases of phishing, email hacking, or interception. The push system, on the other hand, fundamentally eliminates these risks by placing transfer control solely in the hands of the losing registrar, who would initiate and complete the transfer with full registrant consent. This system offers several long-

term benefits: Eliminating the risk of stolen TACs: Unlike a TAC, which can be compromised, a push-based system gives registrants complete control over their assets, minimizing security concerns. Simplified transfer processes: The push system provides registrants with a more direct and transparent process, reducing potential confusion. Scalable infrastructure: Although it may require initial investment, the push system is future-proof and would significantly reduce the need for ongoing patches and security fixes to the TAC system. To address concerns about the feasibility of transitioning to a push system, I propose ICANN consider launching a pilot program with willing registrars to assess the system's effectiveness. This could be implemented alongside the current TAC system, providing registrants with an alternative that can be evaluated empirically. I am happy to collaborate further with ICANN to explore how this system could be introduced gradually, ensuring minimal disruption while improving the long-term security and stability of domain transfers. Thank you for your consideration, and I look forward to engaging further on this important issue.

## Recommendation #5: TAC Definition

Page 12 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #5:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #5, please indicate the revised wording and rationale here.

I would like to take this opportunity to further advocate for the adoption of a push-based transfer system, as fully documented in my company's prior submission: <https://freespeech.com/wp-content/uploads/2022/08/LEAP-comments-Transfers-Phase1a-20220814-FINAL.pdf> which I believe would offer a more comprehensive and permanent solution to transfer-related security issues. While the improvements to the TAC system reduce some risk, the fact remains that any shared-secret mechanism like TAC still presents vulnerabilities, particularly in cases of phishing, email hacking, or interception. The push system, on the other hand, fundamentally eliminates these risks by placing transfer control solely in the hands of the losing registrar, who would initiate and complete the transfer with full registrant consent. This system offers several long-term benefits: Eliminating the risk of stolen TACs: Unlike a TAC, which can be compromised, a push-based system gives registrants complete control over their assets, minimizing security concerns. Simplified transfer processes: The push system provides registrants with a more direct and transparent process, reducing potential confusion. Scalable infrastructure: Although it may require initial investment, the push system is future-proof and would significantly reduce the

need for ongoing patches and security fixes to the TAC system. To address concerns about the feasibility of transitioning to a push system, I propose ICANN consider launching a pilot program with willing registrars to assess the system's effectiveness. This could be implemented alongside the current TAC system, providing registrants with an alternative that can be evaluated empirically. I am happy to collaborate further with ICANN to explore how this system could be introduced gradually, ensuring minimal disruption while improving the long-term security and stability of domain transfers. Thank you for your consideration, and I look forward to engaging further on this important issue.

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

Page 13 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #6:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #6, please indicate the revised wording and rationale here.

I would like to take this opportunity to further advocate for the adoption of a push-based transfer system, as fully documented in my company's prior submission: <https://freespeech.com/wp-content/uploads/2022/08/LEAP-comments-Transfers-Phase1a-20220814-FINAL.pdf> which I believe would offer a more comprehensive and permanent solution to transfer-related security issues. While the improvements to the TAC system reduce some risk, the fact remains that any shared-secret mechanism like TAC still presents vulnerabilities, particularly in cases of phishing, email hacking, or interception. The push system, on the other hand, fundamentally eliminates these risks by placing transfer control solely in the hands of the losing registrar, who would initiate and complete the transfer with full registrant consent. This system offers several long-term benefits: Eliminating the risk of stolen TACs: Unlike a TAC, which can be compromised, a push-based system gives registrants complete control over their assets, minimizing security concerns. Simplified transfer processes: The push system provides registrants with a more direct and transparent process, reducing potential confusion. Scalable infrastructure: Although it may require initial investment, the push system is future-proof and would significantly reduce the need for ongoing patches and security fixes to the TAC system. To address concerns about the feasibility of transitioning to a push system, I propose ICANN consider launching a pilot program with willing registrars to assess the system's effectiveness. This could be implemented alongside the current TAC system, providing registrants with an alternative that can be evaluated empirically. I am happy to collaborate further with ICANN to explore how this system could be

introduced gradually, ensuring minimal disruption while improving the long-term security and stability of domain transfers. Thank you for your consideration, and I look forward to engaging further on this important issue. The prior concern about the ambiguity (as noted in the comment above for Recommendation #3) of "5 calendar days /120 hours" also applies here.

## Recommendation #7: TAC Composition

Page 14 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #7:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #7, please indicate the revised wording and rationale here.

While I appreciate the working group's effort to improve the security of the Transfer Authorization Code (TAC) by aligning it with RFC 9154, I must emphasize that the underlying reliance on a shared secret (such as the TAC) remains fundamentally insecure. As outlined in past submissions, including in the Leap of Faith Financial Services Inc. comments at: <https://freespeech.com/wp-content/uploads/2022/08/LEAP-comments-Transfers-Phase1a-20220814-FINAL.pdf> and those of others, the problem with shared secrets like the TAC is not necessarily in how they are generated, but in how they are stored, transmitted, and handled across multiple systems. Even with enhanced encryption and compliance with standards such as RFC 9154, these tokens can still be intercepted, stolen, or misused—whether through phishing attacks, email compromise, or system vulnerabilities at either the registrar or registry level. ICANN's own history of policy evolution shows that incremental improvements to the TAC system (such as one-time use and time-limited validity) address some aspects of the problem but fall short of eliminating the **\*\*systemic risks\*\*** posed by the shared secret model. Attackers who gain access to the TAC, even for a brief period, can potentially compromise high-value domains. In the banking industry, secure transactions like wire transfers operate on a similar push-based system. When a wire transfer is initiated, the instructions—such as the recipient's account number and bank routing information—are completely public and do not rely on any secret code or token. The security comes from the push mechanism, where the sender's bank initiates the transfer with explicit authorization from the account holder. This eliminates the vulnerabilities associated with shared secrets and mirrors the kind of protection that a push-based transfer system for domain names would offer. The losing registrar, analogous to the sending bank, would have full control and responsibility to authorize and initiate the transfer, thereby significantly reducing the risk of unauthorized transfers. By continuing to rely on a

shared secret, even with more secure composition requirements, the policy still leaves registrants exposed to the risk of domain theft and unauthorized transfers. The only way to fully address this vulnerability is to eliminate the use of shared secrets like the TAC altogether and transition to a model where the losing registrar maintains full control over transfer initiation. Thus, the claimed improvements in Recommendation #7 fall well short of the mark, and I strongly urge ICANN to reconsider the fundamental reliance on the shared secret model and to explore more secure alternatives like the push-based system.

## **Recommendation #8: Verification of TAC Composition**

Page 15 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #8:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #8, please indicate the revised wording and rationale here.

This recommendation demonstrates a fundamental misunderstanding of security by the working group. While the proposal suggests that the registry should verify the “randomness” of the Transfer Authorization Code (TAC), the reality is that this is impossible without direct access to the registrar’s internal systems. For example, a registrar could theoretically use the same hard-coded TAC for all transfers, as long as it satisfies the length requirement. The registry has no way of knowing whether a TAC is truly random or if it is the result of a weak, predictable, or even non-random generation process. The TAC "123456789012345678901234567890," for instance, may meet the 128-bit entropy requirement in terms of length, but the registry has no ability to verify the actual randomness of that code. The only check a registry can perform is whether the TAC meets the length standard, not whether it was generated securely. Without access to the registrar’s source code, algorithms, and hardware environment, the registry cannot ascertain whether the TAC adheres to any meaningful security or randomness standard. Thus, the current recommendation provides a false sense of security, as the registry is only able to verify superficial attributes like string length, which says nothing about the integrity or randomness of the TAC. Indeed, this design flaw allows for vulnerabilities such as hard-coded TACs that could be reused repeatedly, completely undermining the security of the transfer process. This is why the TAC system, as it currently stands, is inherently flawed. The solution lies in moving to a better system, such as the push-based approach used in wire transfers within the banking industry. As outlined in my previous detailed submission, this system does not rely on shared secrets like the TAC and provides far superior protection against unauthorized transfers. In



conclusion, while the intent to improve security by verifying TAC composition is commendable, the approach is inadequate and does not address the fundamental weaknesses of the TAC model. I urge ICANN to reconsider the use of TACs altogether and adopt a more secure, push-based design for domain transfers.

## **Recommendation #9: TAC Time to Live (TTL)**

Page 15 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #9:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #9, please indicate the revised wording and rationale here.

While I acknowledge the rationale behind limiting the Time to Live (TTL) for the Transfer Authorization Code (TAC) to 14 calendar days as a security measure, this recommendation only serves to highlight the inherent security vulnerabilities associated with the TAC system. The underlying concern about "unused TACs" emphasizes the real problem: the potential for the wrong person to gain access to the TAC. The very fact that ICANN is concerned about unused TACs being stored in a registrant's email or other insecure locations illustrates that the TAC system is inherently insecure. If the TAC were never exposed or sent through potentially vulnerable channels, this concern would not exist. The issue here is that shared secrets like TACs are vulnerable to interception or unauthorized access, even with a limited validity period. Rather than adding incremental security fixes like time limits, it would be far better to implement a completely superior design that eliminates the risks associated with shared secrets altogether. A push-based transfer system, similar to those used in the banking industry for wire transfers, would remove the need for TACs and the associated security risks. In a push-based model, the losing registrar initiates and authorizes the transfer, reducing the chance of interception or misuse by unauthorized parties. The rationale behind this recommendation supports my argument: ICANN is rightfully concerned about the potential for unauthorized use of TACs. However, the most effective solution is not to limit the lifetime of an inherently flawed system, but to adopt a more secure, robust design that does not rely on vulnerable authorization codes. I strongly urge ICANN to move beyond patching security gaps in the TAC system and instead explore better alternatives, such as the push-based model, which would eliminate the security concerns surrounding unauthorized access to transfer codes altogether. The prior concern about the ambiguity (as noted in the comment above for Recommendation #3) of "14 calendar dates /336 hours" also applies here.

## Recommendation #10: TAC Generation, Storage, and Provision

Page 17 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #10:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #10, please indicate the revised wording and rationale here.

While I appreciate the working group's effort to introduce more secure practices for the generation, storage, and provision of the Transfer Authorization Code (TAC), this recommendation still fails to address the fundamental flaws of the TAC system itself. As argued in previous submissions, the primary issue is not how securely the TAC is generated or stored, but that the TAC as a shared secret is inherently insecure. The recommendation to improve the security of the TAC by requiring that it only be generated upon request and securely stored at the registry is merely an incremental fix to a deeper problem. Even if the TAC is securely generated and stored, it still relies on transmission through potentially vulnerable channels, such as email, where it can be intercepted or stolen by malicious actors. Moreover, once the TAC is generated, there is a window of vulnerability until it is used. No matter how strong the encryption or how securely it is stored, the fact that the TAC exists as a transferable secret makes it a potential target for attackers. The very need for stronger storage requirements and the concern about securely transmitting the TAC underscores the systemic risk of relying on shared secrets in the domain transfer process. In addition to these security concerns, ICANN should also consider the issue of technical debt. Continuously patching and adding security fixes to an inherently flawed system—like the TAC-based transfer process—leads to accumulating technical debt. Each incremental improvement adds complexity and costs in the form of maintenance, compatibility issues, and further patches. Over time, this technical debt increases the long-term cost of maintaining a system that is fundamentally insecure and poorly designed. Rather than continuing to pour resources into patching these flaws, it would be far more cost-effective in the long run to transition to a cleaner, more secure push-based system. A push system, where the losing registrar directly initiates and authorizes the transfer, would eliminate the need for shared secrets like the TAC altogether. This model would not only reduce the operational complexity but would also minimize security risks, creating a simpler, more robust framework for domain transfers. In fact, adopting a push system could potentially be cheaper than the cumulative cost of repeatedly applying incremental fixes to a flawed system. By addressing the root problem now and migrating to a superior design, ICANN would avoid the compounding costs and risks associated with the TAC model. While the improvements to the TAC process outlined in

Recommendation #10 are a step forward, they are ultimately treating the symptoms rather than addressing the root cause of the security issues. The real solution lies in moving away from the TAC model altogether in favor of a more secure, push-based system, as seen in other industries like banking. I urge ICANN to consider not just securing the TAC better, but to rethink the transfer authorization process entirely, replacing it with a more secure and fundamentally sound approach that reduces both security risks and long-term technical debt.

## Recommendation #11: Notification of TAC Issuance

Page 18 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #11:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #11, please indicate the revised wording and rationale here.

While I understand the intention behind Recommendation #11, which seeks to ensure that the Transfer Authorization Code (TAC) issuance is promptly communicated to the registrant, this approach continues to fall short of addressing the core security risks inherent in the TAC-based system. As I have argued in past submissions, the problem lies not in the notification process but in the TAC system itself. Even with a notification sent within 10 minutes of TAC issuance, the risk remains that the TAC could be compromised before or after the notification is received. This is particularly true when the TAC is delivered through vulnerable communication channels, such as email or SMS, which can be intercepted by malicious actors. Sending a notification after the TAC has been issued is a reactive measure that offers little real-time protection against unauthorized access. The need for this notification, in fact, highlights the inherent insecurity of relying on the TAC as a shared secret. The system remains susceptible to interception and misuse, and a notification only serves as a post-factum alert when the damage may already have occurred. Moreover, these incremental changes—such as adding notification requirements—add unnecessary complexity and technical debt to an already flawed system. By continuing to patch the TAC system with fixes like these notifications, ICANN is only doubling down on an inherently poor design. Every incremental improvement increases technical debt, meaning additional future costs, maintenance, and potential vulnerabilities. Worse, these ongoing fixes will also impose operational costs on registrars, who will need to implement and manage these added security layers without addressing the underlying security issues. Rather than continuing to pour limited resources into maintaining this flawed system, those resources could be far better spent transitioning to a more secure and efficient model. The most sensible

path forward is not to keep piling on new fixes but to stop digging when you're in a hole. Instead of continually reinforcing a fundamentally insecure system, ICANN should focus on shifting to a superior design, such as the push-based transfer system that I have previously advocated. In a push system, the losing registrar directly initiates the transfer, entirely eliminating the need for a shared secret like the TAC and its associated risks. This push-based approach would simplify the transfer process, reduce operational and technical overhead for registrars, and provide significantly better security by ensuring that no sensitive transfer authorization codes need to be passed around or stored insecurely. Instead of burdening registrars with additional notifications and technical requirements to patch vulnerabilities, a push system would allow registrars to focus on more secure, streamlined operations. In conclusion, while the intent behind Recommendation #11 is to improve security, it ultimately adds complexity and cost without solving the core problem. ICANN should use this opportunity to rethink its approach and adopt a more secure, push-based transfer system, reducing long-term technical debt and providing real protection against unauthorized transfers.

## **Recommendation #12: Verification of TAC Validity**

Page 19 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #12:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #12, please indicate the revised wording and rationale here.

While Recommendation #12 maintains the status quo by confirming the necessity for registries to verify the validity of the Transfer Authorization Code (TAC) during the transfer process, it fails to address the fundamental issues with the TAC-based system that have been raised in previous submissions. The fact that the TAC system continues to be relied upon does not mean it is the best or most secure option available. As I have consistently argued, the TAC system is inherently flawed because it depends on a shared secret that is vulnerable to interception, misuse, and theft. Verifying the validity of a TAC is only a safeguard after the fact—once the TAC has already been issued and is circulating. This approach does nothing to prevent the core security risks associated with the TAC, such as interception during transmission or improper access by unauthorized parties. Despite the fact that Recommendation #12 merely reaffirms the current system, ICANN should take this opportunity to consider alternative options that would better protect registrants from the inherent vulnerabilities of the TAC. The status quo should not be seen as the only path forward, particularly when more secure models, such as a push-based

system, are available. A push system, where the losing registrar initiates and authorizes the transfer directly, offers superior security by eliminating the need for shared secrets like the TAC entirely. Instead of relying on a code that can be stolen or misused, the push system ensures that transfers are initiated and controlled by the party that already has established authorization—the losing registrar. This approach would drastically reduce the risks associated with domain transfers. Moreover, it is essential to give registrants and consumers a choice. ICANN should not continue to lock the entire system into a single, outdated method of transfer. I strongly urge ICANN to pilot a parallel push system, allowing registrants the option to use a more secure and efficient transfer method. By running both systems concurrently, ICANN could gather valuable data on the effectiveness of a push system while giving consumers the freedom to choose a more secure option if they prefer. In conclusion, while Recommendation #12 preserves the current practice of verifying TAC validity, it misses an opportunity to address the deeper security concerns with the TAC-based system. By piloting a parallel push-based system, ICANN could offer registrants greater security and choice, ultimately moving the domain transfer process toward a more reliable and secure future.

## Recommendation #13: TAC is One-Time Use

Page 20 of the TPR PDP Initial Report

### 1. Please choose your level of support for Recommendation #13:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

### 2. If your response requires an edit or deletion of Recommendation #13, please indicate the revised wording and rationale here.

While I understand the rationale behind making the Transfer Authorization Code (TAC) a one-time use code as a security measure, this recommendation still fails to address the fundamental weaknesses of the TAC-based system that have been repeatedly highlighted in past submissions. The requirement for one-time use is yet another incremental patch on a system that is inherently flawed. Even with this enhancement, the TAC remains a shared secret that can be intercepted or misused before it is invalidated. Whether the TAC is used once or multiple times does not change the fact that it exists as a vulnerable piece of information during the transfer process. This recommendation only reduces the impact of a compromised TAC but does not eliminate the core risk of unauthorized access. Furthermore, ICANN recognizes the existence of bad actors in the domain space, and this is one of the reasons behind the one-time use requirement. However, bad actors are best handled by eliminating the attack vector altogether, rather than merely reducing the damage they can cause. As long as the TAC exists,

it provides an opening for exploitation. Once a TAC is generated, it can still be intercepted or phished, and the damage could already be done before any one-time use restrictions or notifications take effect. Eliminating the TAC system and moving to a push-based transfer system would close this attack vector entirely, ensuring that bad actors have no opportunity to exploit shared secrets. Moreover, these new requirements come at a cost for registrars, who must now implement and manage additional infrastructure to enforce the one-time use rule. This adds operational complexity and increases technical debt, as registrars must continue to invest in patching and maintaining a system that is fundamentally insecure. Each incremental improvement, such as the one-time use requirement, further entrenches a poor design that will require ongoing resources to maintain and secure. Rather than doubling down on this flawed system, it would be far more beneficial for registrars to direct their scarce resources toward adopting a superior design. A push-based transfer system, as I have advocated previously, would eliminate the need for shared secrets like the TAC entirely. In a push-based system, the losing registrar would directly initiate and authorize the transfer, removing the vulnerabilities associated with the TAC and simplifying the overall process. This would not only provide better security but would also reduce long-term costs for registrars, as they would no longer need to implement frequent fixes and patches to secure a fundamentally flawed system. The continued reliance on the TAC system represents a growing technical debt for registrars and ICANN alike. With each additional layer of security, the system becomes more complex, harder to maintain, and more expensive. Bad actors will always exist, but the best way to mitigate their actions is to remove the opportunity for exploitation—not just limit it. By transitioning to a more secure and efficient push-based system, registrars could free themselves from the constant cycle of incremental fixes and invest in a more sustainable, future-proof solution. In conclusion, while Recommendation #13 introduces another layer of security by limiting the TAC to one-time use, it fails to address the root cause of the system's insecurity. ICANN should take this opportunity to explore a better approach, such as a push-based transfer system, which would provide long-term security and cost benefits for both registrars and registrants. It is time to stop doubling down on a flawed design and focus on building a more secure and efficient system for the future, eliminating attack vectors that bad actors could exploit rather than managing their aftermath.

## **Recommendation #14: Maintenance of Records**

Page 20 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #14:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #14, please indicate the

revised wording and rationale here.

While ICANN's Recommendation #14 regarding transfer logging and record-keeping is a positive step toward improving transparency and accountability in the domain transfer process, it still falls short in addressing the core security risks of the Transfer Authorization Code (TAC) system, as highlighted in previous submissions. The proposal to require registrars to retain records of TAC issuance and usage is a reactive measure that deals with the aftermath of a transfer, rather than preventing security breaches in the first place. This type of logging may assist in forensic investigations after an issue has occurred, but it does little to prevent unauthorized transfers or address the inherent vulnerability of the TAC as a shared secret. As I have argued in the past, the TAC system is fundamentally insecure because it relies on a secret that can be intercepted or stolen. While logging the issuance and use of the TAC may help identify when and how a breach occurred, it does not prevent the breach itself. Additionally, this recommendation continues to double down on a flawed system, adding more complexity without addressing the root problem: the TAC itself. One area that is notably absent from this recommendation is the need for detailed record-keeping by the gaining registrar, particularly with respect to the IP address and other data associated with the entity that applied the TAC. Knowing which IP address or user applied the TAC can provide crucial information in the event of a dispute or investigation, and this data should be included as part of the mandatory logging requirements for the gaining registrar. Without these details, it will be difficult to track down malicious actors or fraudulent transfers. However, even with more comprehensive logging, these measures remain a band-aid solution for a flawed process. The emphasis should be on preventing the attack vector altogether, rather than simply making it easier to investigate after the fact. A push-based transfer system, as I have consistently advocated, would eliminate the need for the TAC and its associated risks. In a push system, the losing registrar initiates and authorizes the transfer, meaning that no shared secrets need to be transmitted, intercepted, or logged in the first place. By moving to a push-based system, ICANN could greatly reduce the need for extensive logging and record-keeping, as the potential for unauthorized transfers would be drastically minimized. The security focus would shift from managing the aftermath of a breach to preventing the breach from occurring. While logging may still be necessary for transparency and accountability, the overall complexity and security risks would be significantly reduced. In conclusion, while Recommendation #14 is a step in the right direction for improving transfer logging, it does not address the underlying flaws of the TAC system. ICANN should also require more detailed record-keeping by the gaining registrar, including IP addresses and other relevant data, but more importantly, it should focus on eliminating the vulnerabilities in the transfer process by adopting a push-based system. This approach would provide better security, lower operational complexity, and reduce the need for reactive measures like extensive logging.

## **Recommendation #15: Maintenance of Records**

Page 21 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #15:

- Support Recommendation as written
- Support Recommendation intent with wording change

- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #15, please indicate the revised wording and rationale here.

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

Page 22 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #16:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #16, please indicate the revised wording and rationale here.

## **Recommendation #17: Losing Form of Authorization (FOA)**

Page 23 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #17:

- Support Recommendation as written
- Support Recommendation intent with wording change



- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #17, please indicate the revised wording and rationale here.

I generally support the intent behind Recommendation #17, but I would like to raise a few important points regarding the language and placement of certain sections within the recommendation itself. First, the first two sentences of the text, namely —"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."—should be moved to the Rationale section, as it is purely commentary and does not belong in the authoritative policy recommendation. This statement provides background information on the working group's deliberations, but it is not a necessary part of the final recommendation text and could cause confusion if left there. The recommendation section should focus solely on the requirements being put in place, leaving the reasoning behind them for the Rationale. Second, as previously discussed in our earlier comments, the use of both "five calendar days" and "120 hours" introduces unnecessary ambiguity into the policy. ICANN should strive for clarity and precision in its recommendations. While the intent is to improve clarity by specifying both calendar days and hours, this approach actually creates confusion, as calendar days and hours are not always perfectly aligned. To avoid any ambiguity, I strongly recommend that ICANN use hours exclusively in the policy recommendation. Specifying timeframes in hours will provide greater precision and ensure that the policy is implemented cleanly and consistently across all registrars. Once hours are defined as the authoritative timeframe, ICANN can reference calendar days in the Rationale or explanatory sections, which do not hold the same level of authoritative weight. This would keep the policy unambiguous while still offering contextual information where needed. The statement in the draft recommendation—"Consistent with the other recommendations in this report, the working group recommends specifying timeframes in both calendar days and hours for greater clarity."—is actually false in practice, as specifying both creates the very ambiguity ICANN aims to avoid. By adopting a clear, hours-based policy in the recommendation itself, ICANN can ensure that the policy is implemented without confusion and is consistent across all registrars. In conclusion, while I support the core of Recommendation #17, I urge ICANN to revise the recommendation text to eliminate ambiguity and ensure the implementation is as clean and precise as possible. Moving commentary to the Rationale and focusing the recommendation on using hours for precise timeframes would greatly enhance clarity and consistency in the policy.

## **Recommendation #18: Transfer Restriction After Inter-Registrar Transfer**

Page 24 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #18:

- Support Recommendation as written

- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #18, please indicate the revised wording and rationale here.

The prior concern about the ambiguity (as noted in the comment above for Recommendation #3) of "30 calendar days /720 hours" also applies here. Use 720 hours, to be precise (and can then use the less precise days in the rationale).

## **Recommendation #19: Notification of Transfer Completion**

Page 26 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #19:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #19, please indicate the revised wording and rationale here.

While I support Recommendation #19 in principle, there are critical details that need to be clarified within the recommendation itself to ensure consistency and usability for registrants, especially in cases where a transfer may be disputed or unauthorized. First, for the item "Date and time that the transfer was completed", it is crucial that ICANN specify whether this time should be recorded in UTC (Coordinated Universal Time) or indicate which time zone is being used. Different registrars and registries may utilize different time zones, which could lead to confusion and inconsistencies in record-keeping. A standard format, such as UTC, ensures that the time is universal and unambiguous, enabling registrants to have a precise reference point. This detail is particularly important in the context of forensic investigations following an unauthorized transfer. Without a clearly defined time standard, registrants may struggle to reconstruct events accurately or pinpoint when a security breach occurred. Furthermore, the language in the recommendation should be amended to move the content of Footnote 10 into

the body of the recommendation itself. As noted previously, footnotes are not considered authoritative, and leaving critical definitions, such as the definition of the “Losing Registrar”, in a footnote risks creating confusion or oversight during implementation. If a footnote is necessary to clarify a term or concept, it is a sign that the term should be fully incorporated into the main text of the recommendation. This will prevent ambiguity and ensure that all parties understand the roles and obligations clearly. Therefore, I recommend revising the recommendation text to incorporate the definition of the “Losing Registrar” directly within the policy language and to establish that the “Date and time that the transfer was completed” should be expressed in UTC, or explicitly specify which time zone is being used. This will provide registrants with clear, consistent, and reliable forensic information in the event of a dispute. In summary, while I support the effort to enhance the clarity and completeness of transfer notifications, it is essential to ensure that key details are captured directly in the recommendation and that all time references are made using a standard format. Doing so will enhance transparency, prevent misinterpretation, and make these notifications far more useful to registrants in the event of unauthorized transfers.

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

Page 28 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #20:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #20, please indicate the revised wording and rationale here.

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

Page 29 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #21:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #21, please indicate the revised wording and rationale here.

We strongly reiterate the concerns raised in our previous submission: <https://freespeech.com/wp-content/uploads/2022/08/LEAP-comments-Transfers-Phase1a-20220814-FINAL.pdf> (starting on page 53 of our August 14, 2022, comments), regarding what was formerly known as Recommendation #19. These concerns remain relevant, and we must once again sound the alarm on this issue. One of the most significant issues here is the capture of the working group. The dominant participation of registrars, who have their own business interests at stake, has resulted in a skewed process. Registrants—who are arguably the most affected by domain transfers and potential abuse—had limited opportunity to participate or influence the direction of these recommendations. This imbalance in stakeholder representation has allowed registrars to assert disproportionate control over the discussions and the outcome, leaving registrants' concerns underrepresented and inadequately addressed. The consequences of this imbalance are especially evident in this recommendation, which proposes changes that could significantly impact registrants without offering them adequate protection or recourse. Changes involving issues of abuse should be considered and examined by an abuse working group, where all relevant stakeholders, including registrants and security experts, have the ability to weigh in on the potential ramifications. Abuse-related policies need thorough scrutiny, and this cannot be achieved in a working group that is overly dominated by one sector of the industry. Moreover, this recommendation conflates the concepts of "evidence" and "proof"—two terms that are not synonymous. As any competent legal expert would confirm, evidence does not equate to proof. Without a clear distinction between the two, the recommendation risks creating a situation where innocent registrants could be falsely accused of abuse based on weak or insufficient evidence. Should this recommendation move forward—despite the concerns raised here and the apparent capture of the working group—it is imperative that the registered name holder must have the right to access all evidence being used against them. Without full transparency and the ability to rebut or challenge such evidence, registrants may be left defenseless, subject to unfair penalties and accusations without due process. Additionally, by referencing section 3.18.1 of the Registrar Accreditation Agreement (RAA)—a document that was negotiated bilaterally between ICANN and registrars—the working group is opening a backdoor for future changes to the definition of "DNS Abuse." The registrars' dominant influence in this working group makes this reference particularly concerning, as it allows for the potential for quiet, unilateral changes to be made to critical definitions without sufficient scrutiny from other stakeholders, including registrants. If adopted, future modifications to the definition of DNS Abuse could be enacted under this policy without the registrant community—or the broader public—realizing the implications until it is far too late. This is precisely why such abuse-related issues should be addressed in a dedicated abuse working group, where these risks can be thoroughly examined by a wider cross-section of the community. The transfer policy working group does not have the appropriate scope or participation balance to make recommendations on these matters. The risk is that, given the fragility of the current system and the limited

understanding that many stakeholders may have of the long-term ramifications of these subtle word changes, these types of policies could quietly shift the balance of power in dangerous ways. Those who tried to push for greater power in the past will likely attempt to do so again, and those knowledgeable enough to fight back may no longer be involved in the future. Therefore, the only responsible course of action is to delete this recommendation in its entirety. It is too risky to allow these changes to move forward in the current form, especially given the imbalance of participation and representation in this working group. In conclusion, Recommendation #21 should be removed entirely. Abuse-related issues deserve focused attention from a more balanced and properly equipped working group. The current process, dominated by registrars, does not allow for adequate representation of registrants' concerns, and this recommendation could lead to serious unintended consequences if adopted. ICANN must ensure that policies protect registrants' rights and that stakeholders have full transparency and due process before any changes are enacted.

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

Page 32 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #22:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #22, please indicate the revised wording and rationale here.

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

Page 34 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #23:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #23, please indicate the revised wording and rationale here.

### **Recommendation #24: Revised Reasons that a Registrar of Record MUST Deny a Transfer**

Page 36 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #24:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #24, please indicate the revised wording and rationale here.

### **Part B: TPR PDP Initial Report - Group 1(b) Recommendations #25–28**

## Recommendation #25: Change of Registrant Data

Page 38 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #25:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #25, please indicate the revised wording and rationale here.

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

Page 39 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #26:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #26, please indicate the revised wording and rationale here.

I have significant concerns with ICANN's Recommendation #26, particularly in relation to

sections 26.2 and 26.3, which propose the removal of crucial language and security measures that directly impact the rights and protection of registrants. 1. Section 26.2: Removal of Key Registrant Rights Language Section 26.2 suggests removing a fundamental provision from the Transfer Policy, specifically Section II.B.1, which states: "In general, registrants must be permitted to update their registration/Whois data and transfer their registration rights to other registrants freely." This statement is not just a procedural note—it is a critical declaration of registrants' basic property rights over their domain names. Domain name registrants rely on the ability to update their Whois data and transfer their registration freely as part of their rights as domain holders. To remove this language would be to obscure a fundamental principle that registrants have relied on for years. It is absolutely necessary that this provision remain explicit within the policy. The suggestion that such rights are implicitly "understood" or can be inferred leaves far too much room for misinterpretation or misapplication by various individuals or groups. Different stakeholders may have different understandings of what these rights entail, and removing this explicit language risks diluting registrants' rights over time. Therefore, this critical statement of registrants' property rights must remain clearly stated in any future policy. 2. Section 26.3: Removal of an Important Security Check Section 26.3 proposes the elimination of an important security check that ensures changes to registrant data are properly authorized. This is a major concern, as this check serves as a preventive measure to verify that any changes made to registrant information are legitimate and authorized by the rightful owner. While Recommendation #27 suggests that notifications will be sent after changes have been made, this is simply insufficient to protect registrants. Post-change notifications cannot prevent unauthorized changes from occurring in the first place. Once unauthorized or fraudulent changes have been made, the damage may already be done, and it can be extremely difficult—if not impossible—to fully reverse the consequences. The security check currently in place acts as a first line of defense against unauthorized changes, and removing it opens up registrants to unnecessary risks. The fact that these checks would be replaced by post-change notifications alone provides registrants with far less protection and makes them vulnerable to domain hijacking or other malicious actions. 3. Conclusion In summary, I strongly oppose Recommendation #26 as currently drafted, particularly sections 26.2 and 26.3. The removal of language that explicitly protects registrants' basic rights, along with the elimination of critical security checks, would significantly undermine registrant protection. These provisions should remain in place to safeguard the interests of domain holders and to ensure the continued security and integrity of the domain name system. I urge ICANN to reconsider these changes and maintain both the explicit property rights of registrants and the essential security checks that protect their domains.

## **Recommendation #27: Change of Registrant Data Notification**

Page 41 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #27:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording



- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #27, please indicate the revised wording and rationale here.

While Recommendation #27 proposes notifying the registrant after changes to their registration or Whois data have been completed, this does not adequately address the security concerns raised in Recommendation #26. As noted in our response to Recommendation #26, simply notifying the registrant after the change has been made is insufficient to protect against unauthorized or malicious changes. The fundamental issue is that by the time a registrant is notified, the change has already occurred, and any potential harm—such as domain hijacking or unauthorized transfer—could already be underway. Reversing such actions can be complex, time-consuming, and in some cases, irreversible. Recommendation #27 does not remedy the problems created by the removal of the important security check in Recommendation #26, which currently serves as a preventive measure to ensure that changes are authorized before they occur. Post-change notifications cannot substitute for the proactive verification mechanisms that safeguard registrants' data and their control over domain assets. We want to make it clear that while notifications after changes are helpful for transparency, they should not be viewed as a replacement for the necessary security checks that were proposed to be removed in Recommendation #26. The two recommendations must be considered together, and the lack of preemptive safeguards in Recommendation #26 makes the notification process outlined in Recommendation #27 inadequate for true registrant protection. In conclusion, while we recognize the utility of notifications, Recommendation #27 does not resolve the critical security risks posed by Recommendation #26. We urge ICANN to reconsider both recommendations in tandem, ensuring that registrants are properly protected before changes are made to their domain registrations, not just notified afterward.

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

Page 43 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #28:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #28, please indicate the

revised wording and rationale here.

While I understand the intent behind Recommendation #28, which aims to mitigate the potential overload of notifications sent to registrants, I believe the approach proposed here is unnecessary and does not belong in the policy itself. Registrants today have numerous tools at their disposal to manage incoming emails effectively, and this issue can be handled more efficiently without imposing additional constraints in the policy. For instance, registrants can easily set up email filters to automatically sort or route these notifications into designated folders, reducing inbox clutter and ensuring that important notices are still received. This is basic functionality that nearly every modern email system offers, and registrants should be taught to utilize these tools rather than having policy accommodate concerns that can be resolved through better email management. Furthermore, if registrars are concerned about sending or receiving thousands of notifications, there are technological solutions available to them. Registrars can consolidate multiple notices into a single email or design notification systems that batch alerts to registrants in a more digestible format. The key issue here is the need to evaluate scarce resources on a cost-benefit basis. Adopting changes like this for edge cases that affect a small number of registrants will impose costs on all registrars if they are adopted as global policy. Every new requirement adds to the technical debt registrars must manage, complicating their systems and consuming resources that could be better allocated elsewhere. Rather than focusing on issues that impact a small subset of users, ICANN should prioritize structural improvements that deliver broad security and operational benefits. For instance, a push-based transfer system—which I have advocated for in previous comments—would address core vulnerabilities in the domain transfer process and provide a greater return on investment for registrars and registrants alike. In conclusion, Recommendation #28 adds unnecessary complexity to the global policy framework, addressing concerns that can be managed at the registrar level without burdening the entire ecosystem. ICANN should focus on solutions that deliver widespread benefits, rather than imposing costs for edge cases that affect only a small number of users. Resources are better spent on meaningful reforms like a push-based system, which would provide long-term security and operational improvements for everyone involved.

## **Part C: TPR PDP Initial Report - Group 2 Recommendations #29–47**

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

Page 45 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #29:

- Support Recommendation as written
- Support Recommendation intent with wording change

- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #29, please indicate the revised wording and rationale here.

While we sincerely sympathize with the operational challenges that registrars, particularly smaller ones, face in managing tight response deadlines, we cannot support Recommendation #29 as currently proposed. This recommendation, which seeks to increase the time for registrars to respond to transfer requests by a factor of six, highlights a broader issue of double standards in ICANN's policies that consistently disadvantage registrants. Registrars have proposed this significant increase in response time to alleviate their operational burdens, yet registrants have never been granted similar accommodations under critical processes like the Uniform Domain-Name Dispute-Resolution Policy (UDRP) or the Uniform Rapid Suspension (URS) system. Since the inception of these policies, registrants have been forced to adhere to rigid and often unrealistic deadlines, with any attempt to revisit or extend these timelines being firmly rebuffed by ICANN. While we have empathy for registrars' needs, we cannot allow this double standard to persist. If registrars are to receive this considerable extension in response time, then registrants must be afforded the same consideration in UDRP and URS disputes. Registrants should be given commensurate increases in their response time, potentially linked to the age of the domain or aligned with internationally accepted norms for responding to disputes, which can often be 60+ days. Without these adjustments, this recommendation unfairly tilts the balance in favor of registrars while continuing to ignore the longstanding burden placed on registrants. Moreover, this working group has been dominated by registrar interests, allowing them to shape the policy in their favor, while registrants and other stakeholders have had limited opportunities to influence the process. The undue weight given to the operational burdens of registrars, while registrants' challenges under UDRP and URS remain ignored, demonstrates an ongoing imbalance in ICANN's decision-making. For instance, as discussed on page 103 of the report, the working group spent considerable time determining the appropriate time limit for initiating a Transfer Emergency Action Contact (TEAC) procedure, settling on a 30-day limit to extinguish that right. Yet under UDRP and URS, complainants are given unlimited time to file a dispute, leaving registrants vulnerable to claims decades after a domain name is registered, with extremely limited time to respond. This double standard is unacceptable. ICANN and registrars cannot cherry-pick reasoning that favors them while failing to apply the same logic when registrants' interests are at stake. We understand and have sympathy for the operational burdens registrars face, but this should not come at the expense of fairness and consistency. ICANN must treat both registrars and registrants with equal consideration. It is unfair that ICANN would move to extend response times for registrars while continuing to deny registrants a similar extension in UDRP and URS disputes, which often place them at a significant disadvantage. In conclusion, we oppose Recommendation #29 unless registrants are provided with similar accommodations in UDRP and URS response timelines. If ICANN is to fix this problem for registrars, it must also address the identical issue faced by registrants. Until this double standard is corrected, we cannot support extending registrar response times without providing registrants the same opportunity. Fairness and consistency must be at the core of ICANN's policies. The prior concern about the ambiguity (as noted in the comment above for Recommendation #3) of "24 hours / 1 calendar day" also applies here.

## Recommendation #30: Timing for Additional Interactions with the TEAC

Page 46 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #30:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #30, please indicate the revised wording and rationale here.

As discussed in the report, the working group has shown a willingness to impose limits on registrar rights, such as capping the time for initiating a Transfer Emergency Action Contact (TEAC) at 30 days. Yet, no such time limits exist for UDRP or URS complainants, who are free to initiate disputes at any time, no matter how much time has passed since the domain was registered. This double standard unfairly burdens registrants, who must be prepared to defend their domain names on extremely short notice, sometimes years or decades after registration. If ICANN is willing to impose limits on registrars, it must apply the same logic to balance the scales for registrants. In conclusion, while we understand the need for greater flexibility for registrars, ICANN must ensure fairness and consistency for all stakeholders. We cannot support Recommendation #30 unless registrants are afforded the same consideration in UDRP and URS processes. It is time for ICANN to address the double standards that have long disadvantaged registrants and ensure that both parties are treated equally under its policies.

## Recommendation #31: Additional Communications with TEAC

Page 47 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #31:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording

- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #31, please indicate the revised wording and rationale here.

While Recommendation #31 attempts to ensure that ongoing disputes between registrars are properly managed, the language fails to account for situations where a dispute cannot be resolved without formal adjudication through a court or other venue. As it stands, the recommendation does not provide the gaining registrar with the ability to "close" a matter, leaving them in a position where ongoing notifications could persist indefinitely without resolution. In real-world scenarios, there will inevitably be cases where a resolution cannot be reached through the standard ICANN procedures, and the dispute must be escalated to a court for a final decision. In such cases, it is unreasonable to expect that email notifications or other forms of communication will continue indefinitely. This creates an unnecessary burden on the gaining registrar and risks cluttering communications with unresolved matters that may never be settled within the ICANN framework. To avoid this, the policy should include provisions that allow the gaining registrar to formally close a matter after a reasonable amount of time or once it has been escalated to an external venue. There must be a mechanism for registrars to end their involvement in a dispute, particularly when resolution is out of their control and lies in the hands of a court or arbitrator. Without this, the policy risks creating a situation where unresolved disputes linger indefinitely, imposing unnecessary administrative burdens on registrars. In conclusion, while Recommendation #31 is well-intentioned, it lacks the necessary flexibility for gaining registrars to close unresolved disputes. The policy must recognize that some disputes will never be resolved within the ICANN framework and provide a means for registrars to end their involvement without being required to continue sending notifications indefinitely. ICANN should revise this recommendation to ensure that the gaining registrar is not left with an unending obligation to manage disputes that have moved beyond their control. The prior concern about the ambiguity (as noted in the comment above for Recommendation #3) of "72 hours / 3 calendar days" also applies here.

## **Recommendation #32: Method of Communication with TEAC**

Page 48 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #32:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted

No Opinion

2. If your response requires an edit or deletion of Recommendation #32, please indicate the revised wording and rationale here.

While Recommendation #32 proposes using email as the primary communication method between registrars for resolving transfer-related disputes, this approach is problematic due to the unreliability of email and the potential for disputes over whether an email was successfully received. Email systems can be affected by spam filters, delivery failures, and other issues that make it difficult to confirm receipt of important communications, especially in high-stakes matters like domain name transfers. Relying solely on email for registrar-to-registrar communications, without any independent and neutral third-party validation, leaves too much room for disputes and uncertainty. One registrar might claim they sent a communication, while the other could claim they never received it, leading to further complications and delays. This is particularly concerning in cases where timeliness is critical for addressing legitimate disputes. Rather than relying on email, ICANN should consider using or adapting an existing centralized communication system for registrars, similar to the recently created Registration Data Request Service (RDRS), which acts as a "ticketing system" for Whois-related matters. A system like this would offer a neutral, verifiable platform for communication, ensuring that messages are sent, received, and logged in a way that both parties can access and verify. This would reduce the likelihood of disputes over whether a message was delivered or received and provide a clear audit trail for communications. By utilizing a centralized system, ICANN can ensure that all communications are documented and tracked through a secure, reliable platform, reducing the risk of miscommunication and improving overall accountability. In the long term, this would create a more efficient and reliable process for handling registrar disputes and transfers, benefiting both registrars and registrants. In conclusion, Recommendation #32 should be revised to incorporate a centralized, neutral communication system rather than relying solely on email. Using a system similar to RDRS would provide the necessary validation and reliability to ensure that registrar-to-registrar communications are properly handled, with less risk of disputes over whether an email was received.

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

Page 49 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #33:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #33, please indicate the revised wording and rationale here.

We strongly oppose the creation of extrajudicial procedures for handling transfer disputes, as proposed in Recommendation #33. Not only does this open the door to potential exploitation and ownership changes without proper due process, but it also places an unnecessary burden on the ICANN community—a community that is already grappling with issues of volunteer burnout. These matters are better left to the courts, which have the structure, expertise, and resources to handle complex ownership disputes fairly. It's important to recognize that we are in 2024, not 1999. The court system is well equipped to handle unauthorized transfers and disputes over ownership, just as it handles property disputes in the offline world. We don't see specialized dispute resolution policies for unauthorized home title transfers, unauthorized copyright transfers, or trademark transfers. These are dealt with through the court system, which offers a robust framework for due process. Trying to create a parallel system for domain transfers is unnecessary and, frankly, a misuse of ICANN's resources. The scale of the problem doesn't justify the extraordinary costs that would be involved in creating a new Alternative Dispute Resolution (ADR) procedure. Domain transfer disputes represent a relatively small number of cases, yet ICANN is considering spending tens of thousands of hours and millions of dollars to set up a process that mirrors what the courts already provide. This would require significant community effort, adding to the burnout already experienced by ICANN's volunteers, many of whom have dedicated years to these working groups. Asking the community to invest this level of energy in creating a parallel system for a limited number of disputes is a misallocation of resources that fails to respect the time and commitment of ICANN's volunteers. Instead of investing heavily in an extrajudicial procedure, ICANN should focus its resources on areas where it can make a tangible difference—improving the security of the transfer process by design. As we've advocated in previous submissions, the development of a push-based transfer system would be a much better use of ICANN's limited resources. This system would address the root cause of unauthorized transfers by making the transfer process more secure, thereby preventing disputes before they occur. The fact that ICANN is willing to dedicate vast resources to creating an ADR mechanism, while neglecting proposals like the push system, which would prevent disputes in the first place, is troubling. ICANN's focus should be on structural improvements that will benefit the entire internet community and prevent the need for ADR in the first place. It makes no sense to build a costly, complex dispute resolution process for a small number of cases, when the courts already serve this function effectively. In conclusion, we oppose Recommendation #33. ICANN should not be wasting precious resources—including community time, effort, and funds—on creating an unnecessary ADR system. The court system already exists to handle these disputes, and ICANN should focus on what it does best: improving the security of the transfer process with initiatives like the push-based system. The community's time and energy are finite, and ICANN should respect that by focusing on solutions that provide long-term value rather than duplicating processes that courts already handle.

## **Recommendation #34: Fees Associated with Voluntary Full Portfolio Transfers over 50,000 domain names**

Page 50 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #34:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #34, please indicate the revised wording and rationale here.

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

Page 51 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #35:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #35, please indicate the revised wording and rationale here.

We oppose the arbitrary \$50,000 bulk transfer fee ceiling proposed in Recommendation #35, particularly when compared to the inconsistent methodologies used by ICANN in determining fees elsewhere—most notably, the Verisign contract for .com domains, where fees are permitted to increase according to a predetermined timetable rather than being tied to actual costs. This discrepancy highlights a double standard in how ICANN approaches bulk transfer fees versus registry fees, which directly impact registrants. It is deeply concerning that this \$50,000 figure has been treated as an immovable price ceiling, seemingly set in stone, despite having no clear relation to the actual costs incurred by the registry to perform bulk transfers. Yet, when it comes to .com domain fees, ICANN has allowed Verisign to raise prices on a regular schedule, a process that does not appear to be based on the real costs of managing the .com registry. This suggests that ICANN is applying one methodology for determining bulk transfer fees while using entirely different methodologies when setting registry fees that affect millions of registrants.



These double standards are unacceptable, and ICANN should be held to the same principles across all areas of pricing. If Verisign is allowed to continue enjoying its monopoly over the .com registry, then ICANN should treat it the same way as regulated utilities are treated in other sectors. Just as electricity providers are subject to economic studies, ratepayer submissions, and regulatory oversight, the pricing structure for .com domains should be scrutinized in the same way, ensuring that fees are tied to actual costs and justifiable by market realities. Alternatively, if ICANN wishes to foster true competition, it should put the .com contract out for regular public tenders, allowing other companies to bid for the opportunity to manage the registry and introduce pricing that reflects the true costs of managing the domain infrastructure. The \$50,000 bulk transfer fee ceiling is nothing more than a historical artifact, with no demonstrable link to the actual costs of performing a bulk transfer. These transfers typically involve little more than running a SQL command or similar processes—far from a complex or resource-intensive operation. Given the simplicity of the task, we argue that bulk transfers should be completely free or, at the very least, that a proper cost study should be conducted to determine what a fair and reasonable fee would be, based on the actual operational requirements. It's important to remember that we're ultimately talking about electronic databases. There is nothing inherently complex or costly about performing bulk transfers, and the costs involved certainly do not justify a flat \$50,000 fee. If this fee is not to be reduced to \$0, then ICANN should commission a comprehensive cost analysis to establish a fee that accurately reflects the true cost of running these operations. To continue with this outdated and arbitrary price is both unfair and unnecessary. In conclusion, we oppose the \$50,000 ceiling as proposed in Recommendation #35. ICANN should work to ensure consistency in how fees are determined across the board, whether for bulk transfers or for .com domain registrations. If Verisign is allowed to maintain its monopoly, fees should be regulated and tied to actual costs, just as they are in other regulated industries. At a minimum, ICANN should conduct a thorough review of the costs involved in bulk transfers and adjust the fee accordingly, as the current figure has no basis in the actual costs of the process.

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

Page 52 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #36:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #36, please indicate the

revised wording and rationale here.

---

## **Recommendation #37: Registry Operator Notice to ICANN of Full Portfolio Transfer Completion**

Page 53 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #37:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #37, please indicate the revised wording and rationale here.

---

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

Page 54 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #38:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #38, please indicate the revised wording and rationale here.

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

Page 54 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #39:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #39, please indicate the revised wording and rationale here.

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

Page 55 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #40:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted

No Opinion

2. If your response requires an edit or deletion of Recommendation #40, please indicate the revised wording and rationale here.

While we have no specific opinion on the content of Recommendation #40, the recommendation suffers from the same issue we have identified elsewhere—namely, that footnotes are not incorporated into the authoritative policy text. This is a fundamental problem because, as stated on Page 4 of the report, “Only the policy recommendation text itself is meant to be considered authoritative.” As such, any critical information relegated to footnotes does not carry weight within the policy framework. If ICANN intends for the information in the footnotes to have real effect, it must be incorporated inline into the recommendation text itself. Relying on footnotes to convey important details or definitions is ineffective, as footnotes are not considered part of the formal policy. Without being explicitly stated in the recommendation, this information will be overlooked or unenforceable in practice. This issue is not limited to Recommendation #40 but affects other recommendations as well—for example, Recommendation #42. To ensure that the policy is clear, enforceable, and aligned with the intended outcomes, ICANN must move the content of footnotes into the main body of the recommendation text. This way, all stakeholders will have a clear understanding of the policy, and the necessary information will be incorporated into the authoritative language of the recommendations. In conclusion, we urge ICANN to address this issue by incorporating the content of footnotes directly into the recommendation text for both Recommendation #40 and other affected recommendations. This will ensure clarity and authority within the policy, avoiding any confusion or misinterpretation about what is and is not enforceable.

## **Recommendation #41: Inclusion of BTAPPA in Transfer Policy**

Page 56 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #41:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #41, please indicate the revised wording and rationale here.

## Recommendation #42: Required Registrar Notification of BTAPPA

Page 57 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #42:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #42, please indicate the revised wording and rationale here.

While we have no specific opinion on the content of Recommendation #42, it suffers from a recurring issue we have raised elsewhere—footnotes are not incorporated into the authoritative policy text. According to Page 4 of the report, “Only the policy recommendation text itself is meant to be considered authoritative.” As a result, any critical information or context placed in footnotes does not carry the same weight or enforceability as the main text of the recommendation. If ICANN intends for the information found in the footnotes to have any real impact or authority, it must be incorporated inline into the recommendation itself. Simply leaving important definitions, clarifications, or instructions in footnotes weakens the clarity and enforceability of the policy. To ensure that the recommendations are fully understood and properly implemented, ICANN should ensure that any information currently in the footnotes is moved into the main body of the text. This is not only an issue with Recommendation #42 but also affects other recommendations, as we previously noted with Recommendation #40. ICANN must take a consistent approach by incorporating footnote content into the primary recommendation text to avoid confusion or disputes about what is or isn’t enforceable under the policy. In conclusion, we encourage ICANN to amend Recommendation #42 by moving the relevant footnotes into the main text. This will ensure that the policy is clear, authoritative, and enforceable across all recommendations.

## Recommendation #43: Domain Name Expiration Dates During BTAPPA

Page 58 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #43:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #43, please indicate the revised wording and rationale here.

### **Recommendation #44: Permitted Rejection of BTAPPA Request**

Page 58 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #44:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #44, please indicate the revised wording and rationale here.

### **Recommendation #45: Required Registration Agreement Language for BTAPPA**

Page 59 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #45:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #45, please indicate the revised wording and rationale here.

### **Recommendation #46: Notice of Registry Fees for BTAPPA**

Page 60 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #46:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #46, please indicate the revised wording and rationale here.

### **Recommendation #47: Prohibition on Post-BTAPPA Transfer Restriction**

Page 60 of the TPR PDP Initial Report

1. Please choose your level of support for Recommendation #47:

- Support Recommendation as written
- Support Recommendation intent with wording change
- Significant change required: changing intent and wording
- Recommendation should be deleted
- No Opinion

2. If your response requires an edit or deletion of Recommendation #47, please indicate the revised wording and rationale here.

## **Part D: Other Comments**

1. Are there any recommendations the TPR PDP Working Group has not considered? If yes, please provide details below.

Yes, the **entirety of our company's prior submission should be revisited in detail:**

<https://freespeech.com/wp-content/uploads/2022/08/LEAP-comments-Transfers-Phase1a-20220814-FINAL.pdf>

Each and every prior recommendation in that submission, which was not seriously reviewed by the working group, should be looked at with fresh eyes.

I am deeply concerned with the misleading claims in the ICANN Transfer Policy Review Working Group Report, particularly on **Page 3**, where it states: **“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.”** This statement is demonstrably false. Upon reviewing the report and comparing it to the documented public feedback, it is clear that **serious submissions were not adequately considered**, and in many cases, they were outright ignored.

This failure to engage meaningfully with the input from stakeholders reflects a **lack of respect**



for the ICANN community. The Working Group's superficial analysis and lack of documentation of key discussions undermine the legitimacy of the report and call into question whether the policy-making process is genuinely collaborative. This is not just a minor oversight; it reveals **systemic issues** in how feedback is handled and how policy is formed.

### **Lack of Documentation and Consideration of Public Input**

To begin, the claim that the Working Group's discussions are "thoroughly documented within this report" is simply untrue. A review of the ICANN wiki, specifically in the **Public Comment Review section** at [Phase 1A - Public Comment Review](#), shows that **numerous serious submissions received no substantive response whatsoever**. In many cases, the **rightmost column**, which is supposed to document the Working Group's response, is left **entirely blank**. This is not a one-off occurrence, nor is it limited to **interim versions** of the report—it appears in **final and current versions** as well. Many stakeholder submissions, including ours, were simply dismissed with vague notations such as **"WG Response: Action Taken: [COMPLETED / NOT COMPLETED]"**, with **no actual action detailed**.

This pattern of ignoring or glossing over stakeholder input is deeply troubling. The **blank responses** not only signal a lack of transparency but also **disrespect the time and effort** that community members put into providing thoughtful, constructive feedback. The entire point of the public comment process is to ensure that the views of the community are heard and that they meaningfully shape the outcome. When substantive input is left unaddressed, it raises serious concerns about whether the Working Group is fulfilling its mandate to consider all perspectives.

### **Specific Examples of Ignored or Superficially Addressed Comments**

One of the most glaring examples of this failure to engage with community input relates to our proposal for a **push-based transfer system**. Our submission outlined in detail how this system would be more secure by design, eliminating many of the risks associated with the current Transfer Authorization Code (TAC) system. Despite the **novelty** and **substance** of this proposal, the only response we received was a brief comment noting, **"The WG has suggested that the CPH TechOps group may want to give further consideration to the operational implications of proposal E."** However, after this vague suggestion, **no further follow-up** was made, and **CPH TechOps never contacted us** to discuss the proposal. This is not what proper consideration looks like, and it certainly does not align with the claim that discussions and disagreements were "thoroughly documented."

Additionally, we submitted proposals for **greater transparency regarding Whois data** before and after domain transfers, so that registrants are able to determine whether a proposed transfer is correct. This suggestion was crucial for improving **registrant protections** and ensuring that any changes to Whois records are fully visible and auditable. However, this, too, was given **no meaningful analysis** in the Working Group's report. It appears that the importance of ensuring transparency in domain transfers was brushed aside, despite the security and operational implications this issue has for registrants.

It is also worth noting that this **pattern of neglect** was not limited to our comments. **Many other stakeholders** saw their input met with similarly **blank responses** or vague notations with no substantive engagement. The fact that **Annex 11** of the report fails to mention **any novel proposals** or innovative suggestions highlights just how much valuable input was disregarded in the process. This omission reinforces the perception that the Working Group was more focused on maintaining the status quo than on truly considering alternative approaches that could improve the transfer process.

### **Misallocation of Resources and Prioritization Issues**

Another issue is how resources and attention were allocated. ICANN has spent **thousands of hours** and **millions of dollars** discussing and refining aspects of the transfer policy, yet crucial proposals that could fundamentally improve the system—such as the push-based transfer system—were not given adequate attention. Instead of investing in **future-proof solutions** that could eliminate many of the security risks inherent in the current system, the Working Group seems content to make minor adjustments that fail to address the core issues.

The current **TAC system** is outdated and exposes registrants to unnecessary risks, yet rather than addressing this with a **bold, forward-thinking solution**, the Working Group has opted for incremental tweaks that do little to improve the overall security or efficiency of the process. **Courts and established legal systems** are far more suited to handling complex transfer disputes than extrajudicial procedures or ICANN-created panels, yet there is a continued push to expand ICANN's scope in ways that are **not aligned with its core competencies**.

### **Conclusion: ICANN Must Improve Transparency and Engagement**

In summary, the Transfer Policy Review Working Group has **not fulfilled its responsibility** to adequately consider and document the input from the ICANN community. The report falsely claims that discussions and disagreements have been thoroughly documented, when in reality, many serious submissions were met with **superficial responses** or outright **neglect**. If ICANN is to maintain its credibility and continue to function as a **community-driven organization**, it must do a better job of respecting and incorporating the input of its stakeholders.

We strongly urge ICANN to **revisit these submissions** with a more thorough and transparent process, ensuring that all proposals, especially those with significant security and operational implications, are given the consideration they deserve. The community deserves a more **open, transparent, and respectful process** where serious input is not just documented but acted upon.

2. Did you find the updated format of the recommendations helpful in your review of the Initial Report?

We have serious concerns with the format, length, and overall presentation of the **Transfer Policy Review Working Group's "Initial Report"**. In reality, this report is **not** an initial document but more accurately a **second report**, and the way it has been presented to the public is both **misleading** and **inadequate**. Furthermore, the report **fails to provide transparency** regarding the responses and suggestions of other stakeholders, creating a bias that favors those who are **"holding the pen"**, typically **ICANN staff and registrars**.

### **Misleading Representation of the Report as "Initial"**

The report is falsely labeled as an **Initial Report**, which misrepresents the stage of the working group's efforts. For many stakeholders, calling a document an "Initial Report" signals that there will be additional opportunities to **engage**, provide feedback, and influence the final recommendations. However, it has become apparent that this is not the case—the Working Group does **not plan to offer the public any further opportunity** to shape the final report before it is submitted to the GNSO Council.

By branding this document as an "Initial Report," ICANN is **misleading observers** who care deeply about these transfer policy issues. Many believe this is only the beginning of the

consultation process, but in reality, this is effectively a **second report**, and it is the last meaningful opportunity for public input. Stakeholders are being deprived of the chance to **substantively influence the final recommendations**, as there will be no additional rounds of public engagement after this point.

### **Unnecessarily Lengthy and Opaque Format**

The **length** and **format** of this report are unsatisfactory. At 152 pages long, filled with **technical jargon** and complex tables, the report is unnecessarily difficult for stakeholders—especially those with **limited time and resources**—to engage with. This imposes a significant barrier to participation, particularly for smaller registrars, community members, and other stakeholders who do not have the capacity to sift through such a lengthy document.

ICANN must recognize that a report of this nature should be **concise, clear, and accessible** to all community members, not just those with the resources to dedicate substantial time to its review. The format of this report discourages participation and skews the policy-making process toward those who are already in a position of influence. If ICANN is truly committed to community-driven policy development, it must make its reports more approachable and user-friendly.

### **Hiding Stakeholder Responses and Competing Proposals**

Another critical issue with this report is the way it **obscures or hides the responses and suggestions** of other stakeholders. This lack of transparency denies the public a fair opportunity to see the range of **competing proposals** that were submitted. By failing to adequately document or present the input of other stakeholders, the report **biases the outcome** in favor of those who are “**holding the pen**,” predominantly **ICANN staff and registrars**.

The result is that alternative proposals, such as those put forward by **registrants** and other community members, are given little to no visibility. This is particularly concerning when it comes to the **push-based transfer system** that was proposed. Despite its potential to vastly improve the security of the transfer process, this proposal was effectively **ignored**, and no meaningful discussion or follow-up was provided. This behavior demonstrates a clear **bias in favor of entrenched interests**, while sidelining proposals that could bring about meaningful change.

By failing to make competing proposals and community feedback **visible** and **accessible** to the public, ICANN is undermining the transparency of the process. This lack of visibility allows those who dominate the process—mainly **registrars and ICANN staff**—to **shape the narrative** without the public being able to see what alternatives were considered, if at all. It also prevents stakeholders from having a meaningful **dialogue** about the strengths and weaknesses of various approaches.

### **Lack of Further Public Engagement**

In addition to these concerns, the fact that the Working Group does not plan to provide the public with further opportunities to engage is deeply problematic. Given the complexity of the issues at hand, stakeholders should be able to **refine** and **influence** the final recommendations. However, the decision to submit the final report to the GNSO Council **without further public comment** closes the door on meaningful engagement.

This is particularly frustrating because important issues—such as the **push-based transfer system**—were not given due consideration. Without another opportunity for public input, the final recommendations will be **pre-determined**, and key concerns about security and fairness in the transfer process will remain unaddressed. **True community-driven policy development**

requires **multiple rounds of engagement**, not a one-and-done approach, especially on issues of this magnitude.

## **Conclusion**

In summary, the Transfer Policy Review Working Group's report is deeply flawed in its **presentation, length, and misleading nature**. By calling this an "Initial Report," ICANN has misled the community into believing that further engagement is possible, when in reality, this is a **second report** with no planned opportunities for additional public input. Furthermore, the **lack of transparency** in documenting and presenting the suggestions and responses of other stakeholders **biases the outcome** in favor of those controlling the report—primarily ICANN staff and registrars.

We urge ICANN to take a more **transparent, inclusive, and accountable** approach to policy-making, where community feedback is not only welcomed but actively incorporated and competing proposals are given the visibility they deserve. ICANN must address these deficiencies before finalizing the report and ensure that all stakeholders have a fair opportunity to shape the outcome.

3. Are there any other comments or issues you would like to raise pertaining to the Initial Report? If yes, please enter your comments here. If applicable, please specify the section or page number in the Initial Report to which your comments refer.

We are submitting this final comment to express our **deep dissatisfaction** with the conduct and priorities of the **Transfer Policy Review Working Group**. It has become abundantly clear that this working group has been **captured** by a narrow set of interests—**predominantly registrars**—while the most affected stakeholders, especially **registrants**, have been effectively **excluded from meaningful participation**. This is not only a gross **misallocation of resources** but a **failure of ICANN's mandate** to serve all stakeholders fairly and equally.

One of the clearest examples of this **misallocation of resources** is the disproportionate focus on **relatively obscure topics** like bulk transfers. From **June 27, 2023, to October 10, 2023**, the working group allocated **13 separate calls** to discuss bulk transfers—a topic of **limited significance** compared to broader, more impactful issues like **transfer security** and **registrant protections**. Meanwhile, **innovative and critical proposals**, such as the **push-based transfer system** we submitted—designed to vastly improve the security of the domain transfer process—were given **minimal attention**. Despite its potential to benefit all parties, particularly **registrants**, this proposal was barely discussed and was brushed aside with no serious follow-up. **Other stakeholder submissions** that would benefit parties beyond registrars received similarly cursory consideration.

This imbalance in attention and resources is simply **unacceptable**. When issues that could significantly improve the **security and fairness** of the system for **all stakeholders** are **ignored or marginalized**, while niche registrar-centric topics receive disproportionate focus, it becomes evident that this process has been **skewed** in favor of **registrar interests**. This is a direct result of **capture**, where those "holding the pen"—primarily **ICANN staff** and **registrars**—are able to shape the agenda and outcomes in their favor, leaving **registrants** and **other stakeholders** out of the conversation.

We submitted our comments in **good faith**, backed by an **established track record** of serious

and substantive input. We participated with the understanding that ICANN's processes are meant to be **inclusive** and **collaborative**, giving equal voice to all affected parties. Yet, time and again, our submissions—and those of others—have been **ignored** or **superficially acknowledged** without any meaningful engagement. This is not how an effective, fair, and transparent policy development process should work.

The failure to allocate resources toward seriously discussing proposals like the **push-based system** is particularly concerning because it speaks to **systemic issues** within ICANN's working group structure. When registrants—the very people who stand to be most affected by these policies—are left out of the decision-making process, it raises serious questions about the **legitimacy** of the outcomes. Registrars and ICANN staff **cannot and should not** be the sole arbiters of these policies, yet that is exactly what has transpired.

This situation **demands systemic reform**. ICANN must **restructure its working group participation** to ensure that **all voices**—especially those of registrants—are adequately represented and that **community proposals** are taken seriously. The working groups should not be dominated by **industry insiders** who have a vested interest in preserving the status quo. Instead, ICANN must ensure that **affected stakeholders** have a fair and equal opportunity to shape policy outcomes.

In conclusion, we urge ICANN to take these concerns seriously and to implement **major reforms** to ensure that its policy-making processes are truly inclusive, transparent, and fair. Registrants and other non-registrar stakeholders deserve to have their voices heard, and we cannot continue to allow working groups to be **captured by a narrow set of interests**. This is **unacceptable**, and ICANN must do better.

By submitting your personal data, you agree that your personal data will be processed in accordance with ICANN Privacy Policy, and agree to abide by the website Terms of Service

<https://www.icann.org/privacy/policy>

<https://www.icann.org/privacy/tos>