34 Burnfield Avenue
Toronto, Ontario M6G 1Y5
Canada

Tel: (416) 588-0269 Fax: (416) 588-5641
Web: www.LEAP.com

Leap of Faith Financial Services Inc.

June 15, 2025

Subject: Transfer Policy Review Working Group Final Report for ICANN Board Consideration - comments

Submitted by: George Kirikos
Company: Leap of Faith Financial Services Inc.
Website: http://www.leap.com/

Dear ICANN Board,

This submission is in response to the call for public comments on "Transfer Policy Review Working Group Final Report for ICANN Board Consideration" as per the notice at:

https://www.icann.org/en/public-comment/proceeding/transfer-policy-review-working-group-final-report-for-icann-board-consideration-28-04-2025

Summary of Key Proposals and Their Core Benefits

Proposal	Core Benefit
"Push-Based" Transfer System	**Eliminates AuthInfo Code (TAC) vulnerabilities, significantly enhances security, simplifies the transfer process, and reduces the risk of domain hijacking.**
Visible "Before" and "After" WHOIS Data in Losing FOA	**Empowers registrants with critical transparency, enabling verification of transfer accuracy and preventing unauthorized transfers to unintended recipients.**

TABLE OF CONTENTS

A. Introduction and Prior Input

The security and stability of the global Domain Name System (DNS) are paramount, directly impacting registrants, businesses, and internet users worldwide. Domain name transfer policies, in particular, represent a critical nexus for these concerns, as vulnerabilities in the transfer process can lead to significant economic and non-economic harms, including loss of privacy, service disruptions, and compromised online assets. This submission to the ICANN Board is therefore presented with a profound recognition of the strategic importance of robust and secure transfer mechanisms.

Leap of Faith Financial Services Inc. ("LEAP"), a privately held company based in Toronto, Canada, possesses a substantial portfolio of approximately 500 domain names, including high-value assets such as school.com, math.com, and leap.com. This portfolio is worth many millions of dollars, establishing a direct and substantial interest in any changes to ICANN transfer policies that could adversely affect the security or rights associated with these digital assets. Beyond its direct commercial interests, LEAP is committed to enhancing the security of all domain names, recognizing that compromises to any online system can have disproportionately large and cascading impacts across the internet ecosystem.

For over two decades, LEAP has maintained an extensive and often unparalleled record of engagement in ICANN policymaking, consistently advocating for the fundamental rights and security interests of domain name registrants. This long-standing commitment is evidenced by a series of interventions that have, in retrospect, frequently been validated by subsequent events or outcomes. Below is a **selection** of our contributions:

- LEAP opposed the abusive monopolist Verisign's proposed monopolistic "Wait Listing Service." Although the ICANN Board ultimately approved it, we feel validated by the fact that the abusive monopolist Verisign never implemented the service, likely due to potential antitrust challenges it would have faced.
- LEAP spearheaded the opposition to the abusive monopolist Verisign's "Sitefinder" system, creating a petition that amassed over 20,000 signatures. Notably, we raised concerns before it even launched. Had ICANN heeded our advice, that controversy could have been avoided.
- LEAP played a pivotal role by sounding the alarm about the proposed registry contracts which would have permitted tiered pricing in .biz, .info, and .org contracts (and which could have then propagated to other gTLDs). This led to a public outcry with thousands of comment submissions opposing

the one-sided contracts, as registry operators' blatant greed and ICANN management's mistake in initially agreeing to such terms was made obvious to everyone. We were vindicated as price caps remained in place, with uniform pricing for all domain renewals.

- LEAP repeatedly defended balanced due process protections for registrants in relation to the UDRP/URS.
- LEAP sounded the alarm about the deeply flawed "Expedited Transfer Reversal Policy" proposal which would have decimated the secondary market for domain names by enabling "sellers' remorse" to reverse legitimate domain name transfers. We worked tirelessly to educate affected stakeholders, and the IRTP-B working group was forced to back down from that flawed proposal.
- LEAP repeatedly opposed the entire new gTLD program (with detailed submissions to the relevant public comment periods). Unlike others who lost substantially via bad investments in new gTLDs, our company was vindicated by its decision to focus on .com domain names. ICANN's predictions, and those of its consultants and "experts" were widely off the mark, worse than even their own "worst case scenarios".
- LEAP opposed the controversial .org contract renewal of 2019 which removed price caps (and the similar proposals for .info, .biz and .asia, as noted on our blog). We were the **only organization** to have **warned ICANN that private equity could take over the .org contract** (point #6 of our submission), and it was only the intervention of the California Attorney General (Xavier Becerra) that forced ICANN to back down from approving the sale of the registry.
- LEAP opposed the final report from the EPDP on Specific Curative Rights Protections for IGOs. While the ICANN Board adopted that report, time will likely again vindicate our thoughtful analysis.
- LEAP repeatedly opposed the renewals of the .com contract with the abusive monopolist Verisign.

This consistent track record of accurate analysis and effective advocacy establishes LEAP's deep expertise and foresight within the complex landscape of ICANN policy development.

The objective of the current submission is to provide expert recommendations for enhancing the Transfer Policy Review Working Group Final Report. While the report contains some positive elements, it falls well short in addressing fundamental security concerns and in incorporating substantive public input, particularly from registrants. These comments, therefore, aim to address the identified shortcomings and propose superior, more secure alternatives, ultimately serving the broader public interest. By leveraging its extensive experience and proven analytical capabilities, LEAP seeks to contribute constructively to the ongoing policy development

process, ensuring that the final transfer policies are robust, secure, and truly reflective of the multistakeholder model.

We submitted input directly to the Transfers Policy working group on multiple occasions, and also posted extensively about transfer policy issues on our FreeSpeech.com blog in order to educate and inform the public. These included:

- Red Alert: ICANN Working Group Wants To Make It Easier To Hijack Domain Names – a blog post (made on July 30, 2022) in advance of the first comment period deadline
- Double Red Alert: Domain Registrars Seek Power Grab To Deny Outgoing Transfers Of Legal Domains They Dislike – a second blog post (made on August 1, 2022) in advance of the first comment period deadline
- Die Hard Opposition To Reduced Security For Domain Name Transfers – a third blog post (made on August 3, 2022) in advance of the first comment period deadline, which compared the current transfer system to **bearer bonds**, rather than a more secure system like **bank wire transfers**
- Making Domain Name Transfers More Secure – a fourth blog post (made on August 9, 2022), in advance of the first comment period deadline
- XPRIZE-style Competition To Improve Domain Name Transfer Security – a fifth blog post (made on August 11, 2022) in advance of the first comment period deadline
- August 14, 2022 comments on Initial Report on the Transfer Policy Review – a detailed **60 page** comment to ICANN, which proposed the "push" transfer system (in Section E starting on page 11), improving the visibility of the destination of the transfer (section G) among other input. Also covered in our August 14, 2022 blog post.
- ICANN75 Session of the Transfer Policy Working Group is Friday at 10:30PM Eastern Time – blog post (made on September 16, 2022) pointing out the superficiality of the working group's review
- September 28, 2024 comments to ICANN – comments on each of the 47 recommendations of the so-called "Initial Report" of 2024 (a misnomer, given that it came after the 2022 report!). Also covered in a blog post of the same day (with a PDF archive).
- Response to ICANN Working Group Regarding Domain Name Transfer Issues – blog post (made on October 9, 2022) responding to an email made on the working group's mailing list made by Theo Geurts (since we're not able to post to the mailing list, as we were not allowed to be members of the working group). We thoroughly rebut his misconceptions about our proposals.
- Registrars Continue To Threaten To Weaken Domain Name Transfer Security – blog post (made on November 28, 2022)

- Visualizing the Security Benefits of the Losing FOA for Domain Name Transfers – blog post (made on November 29, 2022)
- AI-generated Audio Podcast about ICANN Transfer Policy – blog post (made on October 5, 2024) with an AI-generated podcast (via NotebookLM) on transfer issues

Our extensive writings **prevented the Final Report from being even less effective than it currently is**, by highlighting the importance of the "Losing FOA", and how registrars could misuse their "Terms of Service" to prevent the transfer of domains they deem objectionable. **While these were important wins for registrants' rights, they merely raised the grade of the Final Report to a "D-" instead of "F".**

We repeat and reiterate the positions made on September 28, 2024 that were not adopted by the working group. The following sections will highlight two of the most important issues that we prioritize.

B. Breakthrough Proposal: The Push-Based Transfer System

The "push-based" transfer system represents a fundamental paradigm shift with the potential to revolutionize domain name security. The current AuthInfo Code (TAC) system is inherently vulnerable, akin to a "bearer bond" where possession of the code grants ownership, leaving a wide window for attack between its generation and use. This design is fundamentally poor, particularly in real-world, less-than-high-trust environments.

Section E (starting on page 11) of our August 14, 2022 submission to ICANN contains the proposal to adopt a "push-based" transfer system, which would permit the elimination of the "AuthInfo Code" (to be renamed "TAC" – transfer authorization code). We termed it the "Breakthrough Proposal".

Revolutionizing Domain Security by Eliminating the Vulnerable AuthInfo Code (TAC) Entirely

The paramount benefit of the push-based system is its complete elimination of the need for a "secret code" or TAC to facilitate a transfer. This fundamental change eradicates entire classes of vulnerabilities and attacks associated with TAC interception or misuse. The proposed system operates much like a bank wire transfer, where the sender provides a routing address (a "Pending Transfer ID" or PTID) that directs the domain name to its precise, intended destination. In a wire transfer, details like the financial institution, branch number, account number, and account holder name are provided, and no "secret code" is involved; similarly, an attacker gains nothing by knowing the PTID in a push-based system. This inherent design makes the transfer process predictable, safe, and significantly more secure, particularly for high-value domains or transfers involving a change of ownership where sharing a TAC poses considerable risk.

The working group's explicit dismissal of the push-based system, citing a preference for "incremental change" and perceived workload, reveals a systemic bias towards minor adjustments to existing flawed systems, even when fundamental security improvements are proposed. This incrementalist approach prevents ICANN from achieving optimal security and fulfilling its mandate, highlighting the critical need for the Board to intervene and demand a more thorough, open evaluation of breakthrough concepts.

It is noteworthy that the Final Report before the ICANN Board does not include the words "**push**" or "**breakthrough**" *anywhere* in the document. [indeed, it didn't appear in their earlier report, either, so the public had little opportunity to even become aware of other approaches and proposals, see here] A search of their own wiki for the term "push" also found limited results.

https://icann-community.atlassian.net/wiki/search?text=push&spaces=TPRPDP

Similarly for "breakthrough"

https://icann-community.atlassian.net/wiki/search?text=breakthrough&spaces=TPRPDP

This is not consistent with the claim made on **page 1** of the Final Report that:

> This Final Report **also documents the public comments received** on its consolidated Initial Report and the Working Group's subsequent analysis, as well as other pertinent information that provides background, context, and associated rationales for the Working Group's final policy recommendations. (emphasis added)

Page 3 states:

> Links to Charter Questions & Summary Deliberations: The extensive summary deliberations and charter questions are now included in an annex to the report, which significantly reduces the length of the Final Report body but allows interested readers who desire further historical context to easily toggle between the recommendation's tables and the annex where the deliberations can be found.

Following reference links lead to the Public Comment Review tool:

https://icann-community.atlassian.net/wiki/spaces/TPRPDP/pages/103605871/Initial+Report+-+Public+Comment+Review

which claims (in the "Rec 4" tab of the Google spreadsheet)

> The WG noted that this new transfer model was **previously discussed during its Phase 1A public comment review (e.g. see WG meeting 10/11/2022)**, and the WG decided not to pursue this path. As such, the WG will not pursue the push-based transfer model at this time. The WG will continue to consider new comments and ideas.

> The WG will share this push-based transfer proposal with **ICANN Technical Operations** and inquire about its viability. If found viable and practical, this proposal may be considered by a future working group. (emphasis added)

However, according to their own transcript (relevant portion starting on page 11) the working group members were openly making statements like:

> JAMES GALVIN: ...the key point that I'm trying to emphasize here is **we don't have to judge his proposal at all**.....
>
> Now, I'm asserting that we have, just my own personal opinion, and therefore, **I'm comfortable saying no, to what George is proposing, and I don't even have to evaluate what he's proposing.** Because I believe that we have chosen and **move forward with a nice incremental change**, which covers everything that needs to be covered. The problem we're trying to solve.
>
> We've maintained security, and we have enhanced the process, streamlining the process, just as I said there in the chat in a couple of words. So we don't have to judge his thing. What we need to do is consider what concerns does he have and ask ourselves if we have addressed those concerns. That's the discussion to be had. And my opinion is, yes, we have, and therefore, no to George. But others may feel differently. So let's get some consensus on that. Thanks. (p. 21, emphasis added)

In other words, the working group was **prejudiced** against any new ideas, and focused entirely on **incremental** change to a poorly-designed system. Instead of having the option of creating a well-designed system that completely eliminates entire classes of vulnerabilities and attacks, they decided to maintain only the current model. **At no time did they ever seriously evaluate the merits of the proposal, but dismissed it outright, because they felt it was too much work! This is a complete dereliction of their duties.**

The argument of "workload" is entirely inappropriate and reveals a double-standard, since the same working group instead prioritized numerous weeks of meetings on the topic of bulk transfers (a relatively minor issue).

We were never even invited to present the proposal before the working group, or answer the concerns of the working group, because they summarily dismissed it.

During the working group's October 15, 2024 call (after we in the September 2024 comment period reiterated the call to consider a push-based system), **they once again refused to consider the merits of the proposal**! According to the transcript:

> ROGER CARNEY: But before we jump into our work today, I just wanted to mention that, as you noticed when you were reviewing comments, that Leap of Faith Services, George Kirkos, had provided comments on a lot of them. The one thing I'll say is he mentions his proposal of the push transfer model that he introduced to us during public comment and the meeting after public comment closed.
>
> Initial report of Group 1A, **so I don't think that we need to cover that. We covered it when we did our comments process for Group 1A.** I would encourage everyone to look at that again if they haven' looked at it. It's a novel idea, concept that George presented as a push versus the current poll, I would say, model of transfers. But **we don't need to cover those specific comments from George this time because we've already covered them**, and it's the same comments. But he did also provide other comments on a few of the recommendations, so we will take a look at those as we go through each of the recommendations. But we won't dive into any of the **push model concepts as we've already talked about it** and decided to move on from that.
>
> The one thing I'll say on that is at ICANN81, during the Tech Ops session, **I will be introducing the push concept to Tech Ops** to see if there's an appetite for Tech Ops to examine that model and see if there is a viability in pursuing that model as a Tech Ops white paper . And if it does, then we'll work through the early part of next year, ICANN82 and the Contractor Party Summit to flush out a lot of those things.
>
> I just recognized that the last transfer white paper from Tech Ops took a couple years to create, so I think that if it does even exist, it'll take a year to create for everyone to get input on to how something like that would work and the benefits and I guess the pros and cons on that. But again, **we won't have to cover those comments from George.** We'll just mark those as we marked them in our Group 1A comment process, but we will look at his new comments that he provided as we hit on those recommendations. (pp. 1-3, emphasis added)

So, again, they failed to review the merits before, and then claimed that they "already covered it".

They even unilaterally said that they'd take it to "Tech Ops". However, Tech Ops is not a true multistakeholder forum for policy discussion. It simply involves registrars and/or registry operators (i.e. contracted parties of ICANN), to the exclusion of all other affected stakeholders (especially registrants). In essence, the Registrars (who dominated the composition of the working group, as noted in our comment submissions) and other contracted parties would unilaterally evaluate the proposal, giving them a veto over the proposal. **This violates everything that ICANN is supposed to stand for, as it excludes affected stakeholders like ourselves, who would directly benefit from the higher security offered by a push-based system.**

It is now many months since ICANN81, and it would likely surprise no one who has read this far that we have never been invited by "Tech Ops" to present our proposal, or answer concerns about it.

Why does this all even matter?

This comparison clearly illustrates the stark differences and the superior security paradigm offered by the push-based system.

Comparison of Current TAC vs. Proposed Push-Based System

Feature	Current TAC-Based System	Proposed Push-Based System
Security Model	"Bearer bond"-like; possession of code grants ownership.	"Wire transfer"-like; domain routed to specific, intended destination.
Vulnerabilities	Highly susceptible to interception, phishing, social engineering, and misuse of the single, powerful code.	Eliminates TAC vulnerability entirely; attacker gains nothing from knowing routing ID.
User Experience (Registrant)	Requires obtaining and safeguarding a secret code; risk of code exposure during sharing for ownership changes.	Obtains a routing ID from gaining registrar; inputs ID at losing registrar; secure for ownership changes as no secret code is shared.
User Experience (Registrar)	Complexities in generating, validating, and managing secret codes; implementing countermeasures against misuse.	Simpler code as no complex secret code generation or misuse countermeasures are needed; potential reuse of internal push code.
Implementation Complexity	Established, but with inherent security flaws requiring ongoing patches.	Initial development for external interoperability, but potentially simpler overall due to reduced complexity of security

		logic.
Trust Model	High trust required from all parties handling the TAC.	Lower trust required; security is inherent in the routing mechanism, not reliant on secrecy.

Besides the obvious process concerns, where the working group would not even consider serious proposals that didn't fit into their "predetermined outcome", we are convinced (based on 20+ years of experience doing this, with huge success in the domain name industry) that a push-based system would massively improve the security of domain name transfers.

One can go back to Section E of the 2022 comments for the proposal itself, but let's try to understand it more briefly. At present, the AuthInfo Code (or TAC, as it will be renamed) is very valuable for an attacker to obtain. Essentially, anyone who obtains it would be able to transfer the domain name to the registrar of their choice. The "rightful" users of the TAC need to guard it carefully, lest it be misused. **All the working group did was try to make it harder to be misused (incremental improvements).**

Instead, we stepped back and looked at the problem in an entirely different way. **Can we design a domain name transfer system that completely eliminates the TAC? And the answer is "Yes, we can."**

To do a domain name transfer today, the current registrant obtains a TAC from their existing registrar, at time A. Then, the TAC needs to be input at the new registrar, say at time B in the future. Between time A and B, there's a huge window where an attacker can obtain the TAC, and transfer the domain name somewhere else, before the legitimate transfer takes place. There are measure like the "Losing FOA", etc which attempt to reduce the vulnerability, but it's still there. And this matters, because the existing TAC is simply too powerful. **It can be used at any registrar, by any prospective registrant.** This is a **fundamentally poor design**, that only really works in high trust environments. The real world is a dangerous place. We compared this current model to a "bearer bond", as noted above. In finance, a bearer bond is a security where whoever physically holds the bond is the owner. For a domain name transfer, whoever gets a hold of that TAC and uses it first gets the domain name (subject to attempts to minimize the window, make the TAC harder to guess, etc.).

The push-based model **completely eliminates** the need for a "secret code" or TAC to facilitate a transfer. Instead, the registrant obtains a routing

address (we called it a "Pending Transfer ID", or PTID) that routes the domain name to its intended destination. The domain name is essentially just "pushed" directly from the current registrar directly to where it was intended to go. **This is exactly how wire transfers work, in banking.** When one does a wire transfer, the sender has to provide the name of the financial institution it's going to, the branch number, the account number, and even the name of the account holder. What's also evident is that there's no "secret code" in bank wire transfers – details can be entirely public, or put into legal contracts. An attacker gains absolutely nothing by knowing the PTID. Entire classes of attacks are eliminated by this superior transfer architecture. And this isn't just for domain names – "push" is the model for transfers of crypto, and many registrars even use **internal pushes for transfers within a registrar**. Our full proposal also neatly handles the nuances of domains (compared to money transfers). In particular, domain names face a renewal cost at the gaining registrar. Furthermore, one wouldn't want a "bad" domain name transferred to one's account at a registrar (e.g. CSAM domains, TM violating domains, etc.). Our proposal restricts the transfer to a specific domain name, where it's paid for at the gaining registrar (that's why it needs to be initiated at the gaining registrar).

Addressing Common Misconceptions

Concerns that initiating transfers at the gaining registrar constitutes a "radical change" are largely unfounded. Typical registrants already begin their transfer process by engaging with their desired new registrar before obtaining any authorization code from their current registrar. The push-based system merely formalizes this natural workflow, replacing a vulnerable TAC retrieval with the secure input of a PTID at the losing registrar, obtained from the gaining registrar. This approach aligns with existing user behavior and enhances security without imposing an unfamiliar process.

Dispelling Implementation Concerns

Claims of exaggerated complexity and cost for implementing a push-based system, often raised by registrars and registries, are not supported by the evidence. This is not "advanced rocket science" but rather predictable and simpler software than the current TAC-based system, which necessitates complex secret code generation, hashing, and countermeasures against misuse. Furthermore, the advent of AI tools and Large Language Models (LLMs) with "vibe coding" has drastically reduced software development costs and timelines, making such implementations more feasible than ever. Many registrars already utilize internal push-based transfer systems, allowing for significant code reuse and reducing the burden of developing entirely new infrastructure. It is also noteworthy that registrars and

registries routinely develop new code for revenue-generating features, suggesting that prioritizing security, while perceived as a cost without direct revenue benefit by some parties, should be equally feasible. As a transitional measure, the new system could initially be offered as an optional, premium service for those demanding higher security for valuable domain names. Historical precedents, such as the resolution of "add storms" concerns (in the context of expiring domain names) through simple rate-limiting technology, demonstrate that technical challenges often have efficient, cost-effective solutions.

Path Forward: Ensuring Proper Evaluation and Implementation

The working group's unilateral decision to refer the push-based system to "Tech Ops," which is not a true multistakeholder forum and primarily involves contracted parties, is a significant concern. This approach effectively grants registrars and registry operators a veto over a proposal that directly benefits registrants by enhancing security, thereby raising concerns about the principles of multistakeholder governance. To ensure a fair and comprehensive evaluation, the following actionable steps are proposed:

- **Immediate Multistakeholder Review:** The ICANN Board should mandate a dedicated, open working group, inclusive of all affected stakeholders (especially registrants), to thoroughly evaluate the push-based model's technical viability, security benefits, and implementation roadmap.
- **Pilot Program:** Initiate a pilot program with volunteer registrants, registrars and registries to test the system in a real-world environment, gathering practical data on its effectiveness and user experience.
- **Transparent White Paper Development:** If a white paper is deemed necessary for further analysis, it must be developed through a transparent, multistakeholder process, not solely by contracted parties.

C. Enhancing Registrant Transparency: Visible WHOIS Data in Losing FOA

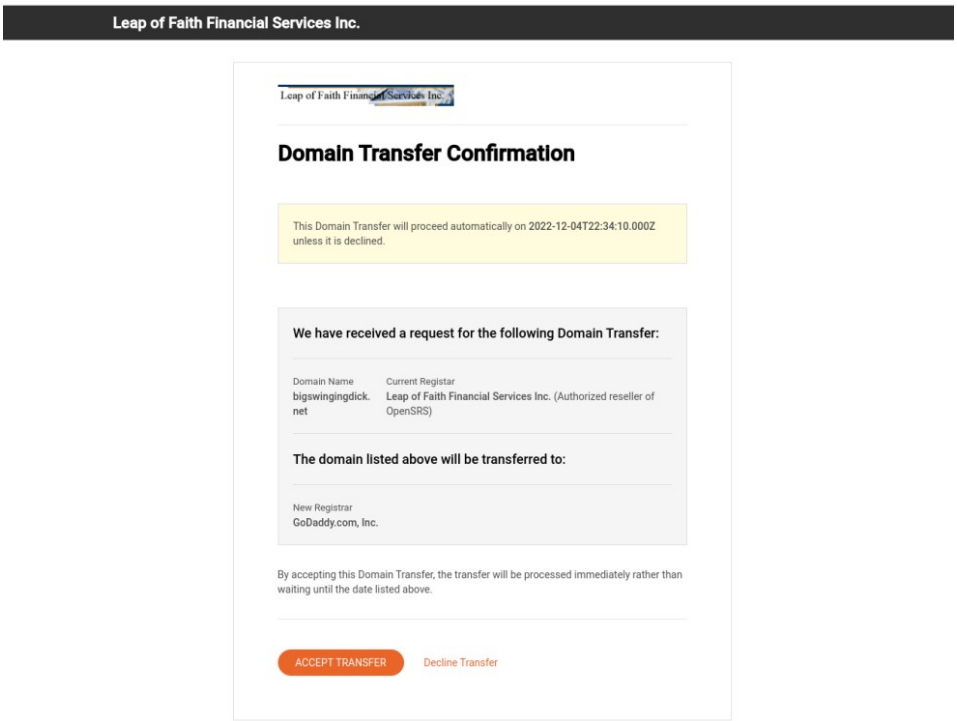
The current system for domain name transfers, particularly the Losing Form of Authorization (FOA), provides insufficient information to registrants, leaving them vulnerable to unauthorized transfers or misdirection.

Empowering Registrants with Unprecedented Transparency and Control

Making the "before" and "after" WHOIS (or registration data) visible as part of the Losing FOA is a critical enhancement that ensures registrants have absolute certainty that a transfer is legitimate and aligns precisely with their intentions, thereby preventing unauthorized changes or misdirection. This empowers registrants with the information they need to make sound decisions regarding their valuable digital assets.

Section G of LEAP's 2022 comment submission detailed the proposal.

Below is a screenshot of a sample Losing FOA, which shows that the domain name will be transferred to GoDaddy:



Registrants deserve to see much more detail in a pending transfer, specifically the full current WHOIS side-by-side with what the future WHOIS would be if the transfer is approved. This allows the current registrant to be absolutely sure that the transfer will make the changes they request, and is not being transferred in an unauthorized manner.

This proposal addresses two major scenarios:

- **Scenario 1 (Self-Transfer to a New Registrar):** When a registrant is simply transferring a domain name to a new registrar under their own ownership, displaying both "before" and "after" WHOIS data allows for immediate, visual verification of the transfer's accuracy. This is a simple, common-sense measure for self-assurance, enabling the registrant to confirm that their data remains correct and the transfer is proceeding as intended.
- **Scenario 2 (Transfer to a New Owner at a New Registrar):** For transfers involving a change of ownership, the need for transparency is even more critical. It is our view that a legitimate new owner would typically be willing to share their WHOIS data with the current registrant, especially when a contract is in place. A reluctance to share this information could indicate potential issues, raising red flags. Furthermore, for corporate new owners, which is often the case for high-value domain names, privacy concerns regarding WHOIS data are frequently moot.

Why does this all even matter?

Under the current TAC-based system, the domain name could be transferred to the intended registrar, but to an ***unintended registrant*** (i.e. the attacker). And so only having the identity of the gaining registrar is insufficient for the existing registrant to have certainty that the transfer is authorized.

Addressing Privacy and GDPR Considerations

We anticipate discussions regarding GDPR and privacy implications. However, our proposal is fundamentally about **empowering registrant choice and consent**. The current approach *denies* registrants the ability to

even express consent regarding the visibility of this crucial information during a transfer. We advocate for an "opt-in" mechanism, allowing registrants (and prospective registrants) to make informed decisions about data sharing, weighing the security benefits against any perceived privacy risks. This aligns with the spirit of modern data protection principles that prioritize individual control over personal data, making it harder to dismiss the proposal on privacy grounds by shifting the focus from "data sharing is bad" to "lack of choice is bad."

Regarding implementation costs, as detailed in the discussion of the push-based system, these are readily solvable technical challenges. Just as senders in bank wire transfers know the full identity of the recipient, the technical infrastructure exists to display this information securely and efficiently within the Losing FOA. The working group's failure to properly consider this proposal further underscores a perceived bias against registrant-centric security enhancements.

D. Concerns about Public Comment Process

We believe that the ICANN public comment periods, while intended to gather input, often fall short of their stated purpose. All public comment periods should be subject to rigorous review to ensure that substantive input is genuinely considered and addressed. The current process can be perceived as merely "going through the motions" without truly incorporating diverse stakeholder perspectives.

The effectiveness of public comment relies on a commitment to reasoned argument and respectful acknowledgment of diverse views, aiming towards consensus policies. However, when significant proposals are dismissed without thorough evaluation, it raises concerns about the integrity of the process itself.

E. Conclusion: Path Forward

The analysis presented herein underscores that the "push-based" transfer system and enhanced WHOIS transparency within the Losing FOA are not merely incremental improvements but represent fundamental shifts necessary for establishing robust domain name security and ensuring comprehensive registrant protection in the evolving digital landscape. These proposals address inherent vulnerabilities in the current transfer policy that the Transfer Policy Review Working Group's Final Report has, regrettably, failed to adequately address.

The working group's dismissal of the push-based system due to a stated preference for "incremental change" and perceived workload reveals a systemic bias within ICANN policy development towards minor adjustments over truly transformative ideas. This incrementalist approach inherently limits ICANN's capacity to achieve optimal security and fulfill its mandate, highlighting the critical need for Board intervention. Furthermore, the dominance of registrars within this working group and the referral of critical proposals to "Tech Ops," which is not a true multistakeholder forum, point to a fundamental challenge within ICANN's multistakeholder model regarding the perceived balance of power and influence. The Board's decision on this report will therefore signal its commitment not only to domain transfer security but also to the integrity of genuine multistakeholder engagement and registrant representation, thereby impacting ICANN's overall legitimacy and accountability.

Therefore, it is strongly urged that the ICANN Board reject the Transfer Policy Review Working Group's Final Report in its current form. The Board should instead mandate further work by a truly multistakeholder body, with explicit instructions to thoroughly evaluate and prioritize the push-based transfer system and the enhanced WHOIS transparency proposal within the Losing GOA. This decisive action would demonstrate a commitment to innovation and prioritize registrant security over incrementalism or the vested interests of specific contracted parties. By taking such a course, the ICANN Board would not only address critical security deficiencies but also reaffirm its dedication to its core mission and the principles of a balanced, accountable multistakeholder model.