Q2 2025

New gTLD Report

Markmonitor™

Q2 2025

Table of Contents

Markmonitor™

Letter From the Editor

The Puck, Ball, and gTLD Stop Here: The Q2 2025 New gTLD Report

As we roll into the middle part of the second quarter of 2025, you find may find yourself "strolling through the park one day, in the merry merry month of May,"[1] or if you are a North American sports fan, you might well find yourself in front of a screen watching a professional basketball or hockey playoff game. The NBA and the NHL playoffs generally start in April and finish in June every year.

For those of you who aren't aware, the National Basketball Association (or NBA) is a "professional basketball league comprised of 30 teams across North America featuring the best basketball players in the world."[2] The National Hockey League (or NHL) is a professional ice hockey league consisting of 32 member clubs with players from more than 20 countries represented.[3]

And with that opening, let's introduce this quarter's Markmonitor gTLD Report with basketball and hockey themes.

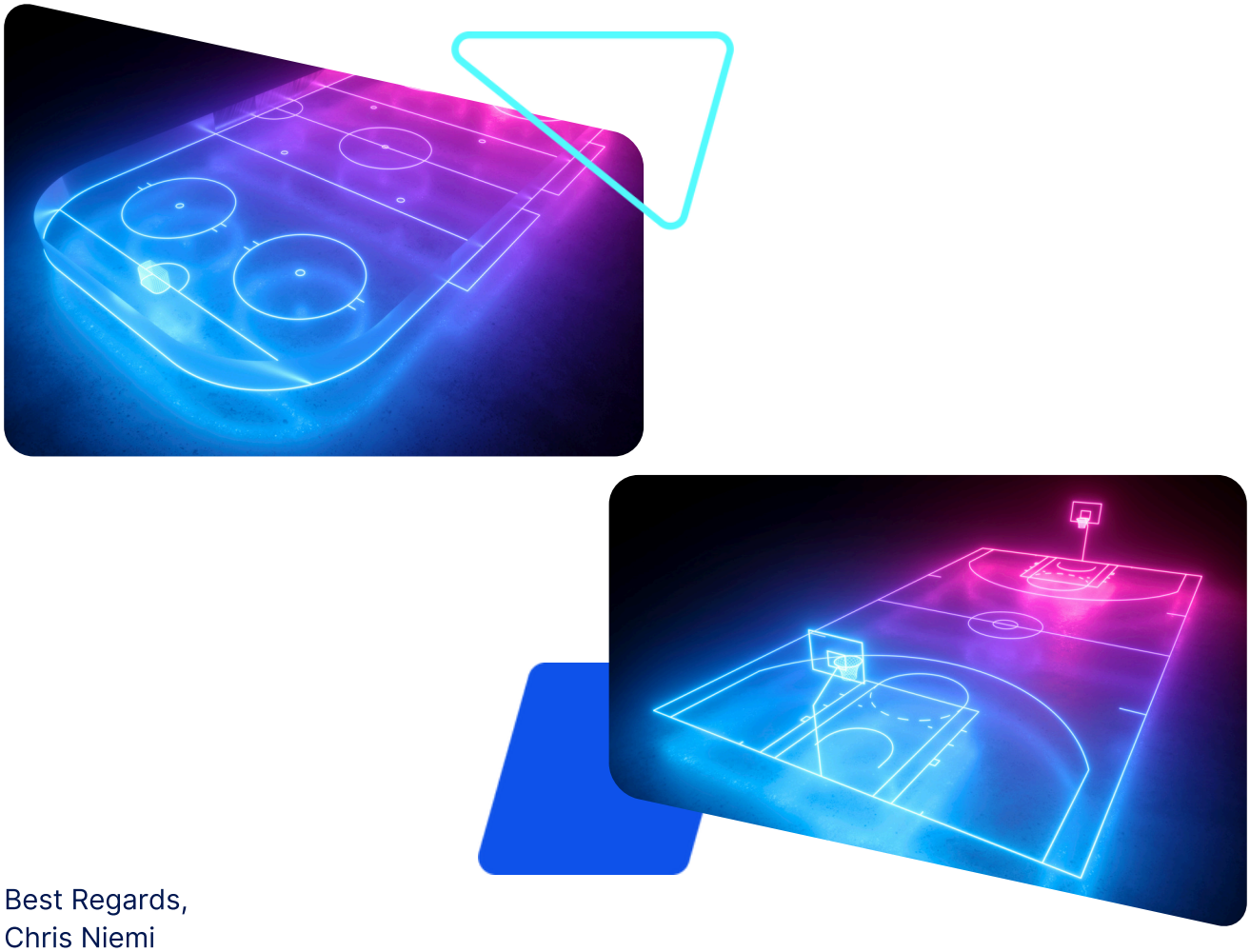
In this month's RSP Spotlight, we learn more about Afnic, the leading Registry Services Provider in France. Did you know that the last two number one overall NBA draft picks were from France? Both Zaccharie Risacher (2024) and Victor Wembanyama (2023) are French.[4]

Our next article is the second in our *Focus on Security* series; in this report, we focus on how the HSTS Preload List can provide a gTLD with important safety benefits. Security in sports can sometimes be hard to quantify, but in both hockey and basketball, a team wants to secure its 'goal' by preventing scoring. As of this writing, the NHL goalie with the highest save percentage (.923[5]), Logan Thompson of the Washington Capitals, has his team still active in the playoffs. Likewise, while the NBA Defensive Player of the Year (DPOY) isn't announced until further along in the playoffs, the reigning 2023-24 DPOY,[6] Rudy Gobert of the Minnesota Timberwolves, has helped his team into the second round of the playoffs.

Our last piece this quarter is in our New gTLDs 101 column, where we discuss the definition of 'name collision' and what effects it can have on the gTLD application process. The most collisions in hockey may well be taken by defensemen, with it being a contact sport, so let's give Ryan Suter of the St. Louis Blues his due, as the oldest player in the league[7] at age 40, he just watched his team get eliminated in the first round.

We'll also wrap up our Q2 New gTLD Report with our usual update on the next ICANN meetings to come.

And with that intro, I wish you an enjoyable read and a successful playoff season!



Best Regards,
Chris Niemi
Manager, Strategic Iniatives

Registry Service Providers: In the Spotlight

The domain industry has a number of members who perform different functions in respect to Top-Level Domains (TLDs). One of these important parties is the Registry Service Provider (RSP), also sometimes known as the BackEnd Registry Operator (BERO). In our RSP Spotlight series we'll introduce you to some of these key industry players.

In this quarter's spotlight we interview: afnic Internet made in France

Emilie Turbat
Chief Marketing and Sales Officer
Afnic

Chris Niemi
Manager, Strategic Initiatives
Markmonitor

RSP Definition:

In the RSP Handbook,[1] a 'main RSP' is defined as:

> A Main RSP is responsible for the registrations of domain names and the reporting functions associated with domain registration. A Main RSP will operate a domain registration database, conduct data escrow and reporting operations regarding those registrations, operate Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) services, and conduct other functions as required by ROs through their agreements with ICANN[2].

Editor's Note: For our purposes, we are referring to RSPs in this 'main RSP' context only; there are other RSP types — DNSSEC, DNS, and Proxy — but those are outside of the initial scope of this series.

So, with that definition, let's get into a real-world example of an RSP and what it does, with our guest, Emilie Turbat, Chief Marketing and Sales Officer at Afnic.

Afnic RSP Spotlight: Interview With Emilie Turbat

■ **Chris Niemi (CN):** Hi Emilie, thank you for taking the time to talk with me. What is your role, and how long have you been in the domain industry?

▲ **Emilie Turbat (ET):** Hello Chris, thank you for inviting me. I value our long-term partnership with Markmonitor, so it is a real pleasure to speak with you today.

I joined Afnic and the domain name industry 16 years ago. Since then, I have been overseeing customer relations — working closely with registrars and registry operators — along with leading our sales and marketing strategy.

I was actively involved in the previous new gTLD round, supporting the launch of major French brands' gTLDs, like .leclerc or .total.

■ **CN:** How long has Afnic been active in the domain industry?

▲ **ET:** Afnic is a not-for-profit organization founded in 1997 to manage the French country code Top-Level Domain, .fr.

Today, we operate 20 TLDs representing over 4.3 million domain names. We handle everything from technical operations and abuse mitigation to customer service, sales, and marketing for six French ccTLDs, the geoTLD .paris, and the 'legacy' community gTLD .museum.

We also serve as the designated Registry Service Provider (RSP) for six brand gTLDs, two ccTLDs, one community gTLD, and three geoTLDs.

This gives us a comprehensive, 360-degree perspective on what it means to run a domain name registry.

■ **CN:** With Afnic's long involvement with running many country code top-level domains (ccTLDs) as well as a number of new gTLDs, can you describe how that experience has helped your service offering improve or change over time?

▲ **ET:** Afnic's mission is one of public interest: contributing every day to a secure, stable, and innovative internet.

This commitment drives us to invest in research and development and to actively engage in global internet governance — helping shape the standards and policies of tomorrow.

Our DNA, combined with the steady expansion of our customer base, compels us to offer top-tier security features and resilient infrastructures. This includes our ISO 27001 certification and our designation as an Essential Service Operator under the NIS (Network and Information Systems) Directive.

Long before the General Data Protection Regulation (GDPR) came into force, Afnic had already been deeply engaged in personal data protection and abuse mitigation. We have also developed innovative dispute resolution services tailored to .fr registrants.

We are committed to ensuring that the expertise we have built in these areas benefits all our customers across all the TLDs we operate.

The onboarding of new gTLDs has been a catalyst for major progress in our Shared Registry System (SRS). We completely redeveloped our system to make it highly performant and scalable. Since 2022, all the TLDs we manage have been migrated to this new system, benefiting from its enhanced capabilities. What has not changed is that our SRS is entirely developed in-house by our tech experts, operated and monitored by our teams, and hosted on our own infrastructure — with the newly added option of hosting it on the SecNumCloud[3] cloud server of your choice.

CN: Now that we know a bit about Afnic's history, what does a BERO/RSP actually do, and why is it important?

ET: Once ICANN approves the application of a new registry operator, it's the Backend Registry Operator (BERO) that makes everything ready for the opening phases and brings the new gTLD to life. The BERO handles all the necessary technical declarations to ICANN and the IANA, ensuring that everything is ready for a smooth launch. When the time comes, it's simply a matter of "pressing the button" to publish the first domain names and activate the new gTLD's infrastructure.

From that point on, the BERO plays a central role in the day-to-day operation of a gTLD, acting as the main point of contact with ICANN to meet service-level requirements and ensure policy compliance. It transmits zone data daily to the escrow operator, serves up WHOIS/RDAP results, provides the technical interfaces needed by the registry operator and its registrar to manage the gTLD and its domain names, and provides operational support throughout the gTLD's lifecycle.

In short, the BERO is the keystone of a gTLD.

> Internet users, increasingly alert to cyber risks, are highly receptive to the tangible security benefits that dotBrand gTLDs can offer — especially when it comes to clearly identifying the brand behind a URL.

CN: Afnic has done extensive research on dotBrands and new gTLDs in the French market. Can you provide our readers with some insights into what you are seeing with French internet users?

ET: In September 2024, Afnic commissioned an independent nationwide survey to assess public awareness and perception of dotBrand gTLDs as well as their perceived value. The goal was to "learn from the other side" — and the insights did not disappoint.

One of the key takeaways was that internet users, increasingly alert to cyber risks, are highly receptive to the tangible security benefits that dotBrand gTLDs can offer — especially when it comes to clearly identifying the brand behind a URL. Among the top perceived advantages were the protection of online transactions and the reduced risk of phishing.

To see the full results of the survey on Afnic's website, click this link.

CN: Before we wrap up, is there anything else you'd like to share with our readers?

ET: I sincerely hope that many brands will apply for their own gTLD in the upcoming application round. A dotBrand gTLD can be a powerful asset for any digital strategy — offering significant advantages in terms of security, brand authentication, distinctive communication, and opportunities for innovation.

Thank you so much, Chris, for the opportunity to talk about a topic that is so special to me.

CN: You are most certainly welcome, Emilie; it was great to get your perspective. We appreciate you sharing your experiences and learning more about how an RSP can touch ccTLDs, policy, and technology!

1. newgtldprogram.icann.org/en/application-rounds/round2/rsp/handbook
2. newgtldprogram.icann.org/sites/default/files/documents/rsp-handbook-03jun24-en.pdf; Section 1.3.1, p.7
3. cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud

Focus on Security: **Can the HSTS Preload List Score for dotBrands?**

Our latest installment of the *Focus on Security* series reviews the HSTS Preload List, a security measure that can be implemented at the gTLD level to protect a dotBrand owner's online assets and reputation.

What is the HSTS Preload List?

This list is “a facility whereby web site administrators can have User Agents (in this case, a HTTP client application typically actively manipulated by a user) pre-configured with HSTS Policy for their site(s) by the User Agent vendor(s) — a so-called "pre-loaded list" — in a manner similar to how root Certificate Authority certificates are embedded in browsers "at the factory."[1]

Before we go further, let’s discuss the HSTS part – that is, HTTP Strict Transport Security.

What is HSTS?

HTTP Strict Transport Security (HSTS) is a simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a website over HTTPS. HSTS exists to remove the need for the common, insecure practice of redirecting users from http:// to https:// URLs.[2]

For a quick digression, HTTPS is hypertext transfer protocol secure, or a “more secure version or an extension of HTTP… <where> the browser and server establish a secure, encrypted connection before transferring data.”[3] HTTPS has security, authority, and performance and analytics benefits over HTTP,[4] so using it can lead to a better experience for end users.

Now, back to HSTS: the idea was proposed in 2009, was adopted by several major web browsers, and finalized as RFC 6797 in 2012.[5]

Per the RFC[6]:

> HSTS is concerned with three threat classes: passive network attackers, active network attackers, and imperfect web developers.
>
> **Passive Network Attackers:** When a user browses the web on a local wireless network (e.g., an 802.11-based wireless local area network) a nearby attacker can possibly eavesdrop on the user's unencrypted Internet Protocol-based connections, such as HTTP, regardless of whether or not the local wireless network itself is secured.
>
> **Active Network Attackers:** A determined attacker can mount an active attack, either by impersonating a user's DNS server or, in a wireless network, by spoofing network frames or offering a similarly named evil twin access point.
>
> **Imperfect web developers:** The security of an otherwise uniformly secure site (i.e., all of its content is materialized via "https" URIs) can be compromised completely by an active attacker exploiting a simple mistake, such as the loading of certain file types over an insecure connection.

Some additional clarity on how HSTS protects users from attacks done by an on-path attacker follows[7]:

> **Browsing history leaks:** : If a user clicks on an HTTP link to a site, an on-path network observer can see that URL. If the site has an HSTS policy that is enforced, the browser upgrades that URL to HTTPS and the path is not visible to the network observer.

Protocol downgrades: If a site redirects from HTTP to HTTPS, an on-path network attacker can intercept and re-write the redirect to keep the browser using plaintext HTTP.

Cookie hijacking: On HTTP requests, an on-path network attacker can see and modify cookies. Even if the site redirects to HTTPS, the on-path attacker can inject cookies into the redirect response.

HSTS Preload List Functionality Across Browsers

The HSTS mechanism works by having sites send a Strict-Transport-Security HTTP response header to a web browser containing the site's policy.[8] Chrome is a browser that maintains a list of domains that have a strong HSTS policy and are HTTPS only, and this "preload list" is built into Chrome.[9] HSTS is supported by major browsers like Firefox, Safari, Opera, and Edge.[10] Other browsers also support HSTS.[11]

dotBrand Domains and the HSTS Preload List

While a domain can be added individually to the HSTS Preload List, an entire TLD can be preloaded as well:

Owners of gTLDs, ccTLDs, or any other public suffix domains are welcome to preload HSTS across all their registerable domains. This ensures robust security for the whole TLD, and is much simpler than preloading each individual domain.[12]

What Brands Have Loaded Their gTLDs Onto the HSTS Preload List?

At this time, global tech giants are taking the lead in this area with the following companies having loaded many of their gTLDs to the 'List:'

- Amazon: .amazon, .fire, .prime, and others
- Google: .chrome, .google, .youtube, and others
- Microsoft: .bing, .microsoft, .xbox, and others

Why Did They Add Their gTLDs to the HSTS Preload List?

At the recent ICANN82 Community Forum, Amazon presented at the public ***GNSO: RySG BRG Membership Working Session*** and Corporate Counsel Christina Bedor said, "... we added all of our dotBrands to the HSTS Preload List, and that was at the recommendation of our security team."[13]

Why Should You Care About the HSTS Preload List?

HSTS is a proven security standard that has been in place since 2012. It protects end-user experiences on the internet by ensuring that their browsers always connect to a website over HTTPS, and secure online experiences build reputational goodwill for brands.

It is available for use on legacy gTLDs, ccTLDs, and new gTLDs. As such, this is a security measure that can be utilized on gTLDs that applicants are awarded in the ICANN New gTLD Program: Next Round (expected to open in 2026).[14] Applicants for dotBrand gTLDs who become registry operators will want to consider listing their dotBrand gTLDs on the HSTS Preload List to improve their overall security posture.

If you would like to talk about the details and security benefits of the HSTS Preload List or applying for your own dotBrand gTLD of tomorrow, please contact your Domain Portfolio Advisor. Markmonitor will continue to watch the space over time and see what dotBrand holders adopt adding their gTLDs to the HSTS Preload List.

Join us next time in our *Focus on Security* series, where we will discuss other security tools that can be used to increase security coverage for dotBrand gTLDs that you currently own or may manage in the future.

1. datatracker.ietf.org/doc/html/rfc6797
2. https.cio.gov/hsts
3. aws.amazon.com/compare/the-difference-between-https-and-http
4. Ibid
5. https.cio.gov/hsts
6. datatracker.ietf.org/doc/html/rfc6797
7. hstspreload.org
8. Ibid
9. Ibid
10. chromium.org/hsts
11. caniuse.com/stricttransportsecurity
12. hstspreload.org
13. icann82.sched.com/event/1vpcl/gnso-rysg-brg-membership-working-session
14. newgtldprogram.icann.org/en/application-rounds/round2

New gTLDs 101: Name Collision in the New gTLD Program

The Internet Corporation for Assigned Names and Numbers (ICANN) ecosystem and community have a wealth of associated acronyms and terminology.

In our *New gTLDs 101* series, we review some of these key terms to help you understand their meaning and how they affect the New gTLD Space.

When Worlds Collide: Name Collision in the New gTLD Program

Per ICANN, the concept of name collision refers to:

> when an attempt to resolve a name used in a private name space (e.g. under a non-delegated Top-Level Domain, or a short, unqualified name) results in a query to the public Domain Name System (DNS). When the administrative boundaries of private and public namespaces overlap, name resolution may yield unintended or harmful results.[1]

For a hypothetical example of this, think of Bob (not his real name). Bob sets up a home network and sets up a server connected to his printer called bob.print that only he has access to — a private space. He uses that space all of the time, and life is grand. Then, ICANN allows the delegation of a new gTLD called ".print."

Domains on the .print gTLD are now a public space. If another party registers the actual domain name bob.print and activates it in the DNS, Bob could have a challenge, as the next time he tries to go to bob.print, his computer may go to the external bob.print website instead of his internal server. This connection could be a problem if the bob.print domain registrant decides he'd like to collect the credentials or files that Bob just sent him and then use them for purposes that Bob doesn't like.

This is an example of a 'name collision,' and depending on the nature of the information that is shared and who receives it, it can become a big issue.

Name Collision and the New gTLD Program

As one might imagine, name collision has been an issue for some time with the rollout of gTLDs and ccTLDs going back into the mid-1980s, but it became particularly important during and shortly after the 2012 New gTLD Program application round as the gTLD namespace was expanding by an exponential amount at that time.

Select Name Collision History (c. 2010–2014)

Adjacent to this time frame, the ICANN community touched the issue in the *SAC 045 – Invalid Top Level Domain Queries at the Root Level – Report* (published November 15, 2020),[2] wherein the ICANN Security and Stability Advisory Committee (SSAC) called attention to the potential problems that may arise from name collision in this report.[3]

In 2013, activity in this area ramped up and after various ICANN Board resolutions, meetings, studies, announcements, and development of documents, ICANN determined a 'Required Change' needed to occur to Specification 6 of the ICANN Registry Agreement (RA; which registry operators for gTLDs had to sign), and this resulted in an updated RA[4] on October 13 of that year.[5]

Continued activity by the community throughout 2014 resulted in the development and publication of the *Name Collision Occurrence Management Framework*[6] on August 1.[7]

Changes to the Registry Agreement (RA)

Name collision was addressed by the RA changes as follows[8] (ideas are simplified; for greater detail, please see the RA wording directly):

- A "No-Activation Period" was created in the 120-day period following the signing of the RA, during which a registry operator could not activate any domain names in the gTLD's zone.
- The idea of a *Name Collision Occurrence Assessment* was created; essentially, this was a report that was based on "analysis of DNS including 'Day in the Life of the Internet' data maintained by the DNS Operations, Analysis, and Research Center (DNS-OARC)."
    - The report determined if the registry operator could implement mitigation measures prior to activating a name or block the activation of second-level domains (SLDs) that hadn't had mitigation measures implemented.
- Name Collision Report Handling would now be required within the first two years after delegation of the gTLD to ensure that the registry operator could receive reports from ICANN of domains that were demonstrating "severe harm from collisions" that could then be removed from the gTLD zone for up to two years so changes could be made in the affected systems.

Name Collision Occurrence Management Framework

The Name Collision Occurrence Management Framework added the following additional components to its name collision mitigation concept[9] (ideas are simplified; for greater detail, please see the framework wording directly):

- Implementation of a 'Controlled Interruption' period "of, at least, 90 days… [wherein] ICANN will monitor and time the implementation of the measure, primarily using the zone files that are transferred to ICANN from new gTLD registries once they are delegated." As part of the controlled interruption period, ICANN will extend a temporary waiver and allow for the use of wildcard DNS records by the registry operator for this period.
- ICANN will allow for insertion of selected DNS records on domains in its 'SLD Block List' for registry operators that were delegated prior to a specific day or ICANN's choosing and activated in the DNS for the 90-day window.
- ICANN limited the "emergency response for name collision reports to situations where there is a reasonable belief that the name collision presents a clear and present danger to human life."

So, taking all of that into account, plus a few more activities, name collision was basically 'baked' as a concept into ICANN by the end of 2015. Generic TLDs that were awarded, contracted, and delegated from the 2012 round generally followed these requirements to mitigate name collision as much as possible.

The 2026 New gTLD Program Next Round and Name Collision

We know a next round is coming — what do we know about any changes for name collision?

Editor's note: As the Subsequent Procedures Implementation Review Team continues to drive the development of the Next Round Applicant Guidebook (AGB*) there will likely be some variation in how name collision processes are defined; for an example see the proposed* ***Topic 29: Name Collision***[10] *proposal, submitted as part of ICANN's recent* ***Fourth Proceeding for Proposed Language for Draft Sections of Next Round AGB***[11] *Public Comment. The details below are based on this proposal. Later this year, we should have a finalized version of the Name Collision section of the AGB.*

- Applicant Access to Longitudinal Risk Data: "Before the opening of the application submission period, ICANN org will provide applicants with datasets related to all strings above a certain threshold of query volume that may help applicants to assess the risk of Name Collision."[12] This may assist applicants in making decisions around any specific name collision risks.
- Initial Assessment of Applied-for Strings: "Each applied-for string (and any variants) will undergo the Name Collision Initial Assessment ("Initial Assessment") using relevant data sets… [whose purpose is to] preliminarily identify high-risk strings."[13] The Initial Assessment will occur after 'string confirmation day,' and ICANN will provide a report after it is completed.

- **Temporary Delegation and Final Assessment:** "Strings (including variants) that are not identified as high-risk during the Initial Assessment" will enter a 'temporary delegation' period where the applied-for-gTLD string will be delegated to DNS nameservers managed by ICANN, using various data points to determine if the gTLD will be designated as high risk and then either be removed from the zone *or* be eligible to proceed with the remainder of application processing. ICANN will provide a report after the period is completed.[14]
- **The Collision String List:** "ICANN org will maintain a Collision String List, which is a list of strings that ICANN has determined to present a high risk of Name Collision."[15]
- **High-Risk String Mitigation Plan Evaluation:** "The applicant for a string on the Collision String List that has cleared contention may amend their application to add a High-Risk String Mitigation Plan". The plan will require various changes to the applicant's application and has certain requirements it must include; the mitigation plan will be evaluated by a panel of technical experts who can advise on possible improvements and required activities that will need to be implemented.[16]
- **Challenges to the Mitigation Plan Evaluation:** The applicant will be given the opportunity to challenge the outcome of a Mitigation Plan Evaluation in certain circumstances; "the deadline for filing a challenge will be within 21 days from the date the applicant receives notice of the evaluation determination it seeks to challenge."[17] Conclusions from the challenge and its final results will be publicly posted.
- **Interaction with Variants:** All applied-for primary gTLD strings, including the applied-for allocatable variant labels, will be assessed for Name Collision risk through the described processes; high-risk strings or variants could have different mitigation outcomes.[18]

Why Does Name Collision Matter for Brands?

The concept of name collision remains intact from the 2012 round; the changes proposed so far for 2026 primarily focus on the foundation of the prior Name Collision Occurrence Management Framework while adding more well-defined processes that are set up before the application round opens. In

this way, applicants will have a better understanding of initial assessments, mitigation plans, and other related matters, so they can better predict and prepare for whether their gTLD strings may qualify as high-risk and then act accordingly throughout the actual application process.

As a company that may be considering applying for a gTLD(s) in the Next Round, understanding name collision is a good practice, as there is a non-zero chance that a potential gTLD string may be high-risk, which could affect the outcome of an application. With that said, of "approximately 1,400 unique strings that were applied for during the last round, only three (.corp, .home, and .mail) were assessed to be high-risk,"[19] so the overall application risk may well be low.

And with that, we've learned about another term in our *New gTLDs 101* series: name collision. Join us next time to learn more information about the domain industry, and don't hesitate to reach out and let us know if there is an abbreviation, acronym, or initialism you'd like to learn about!

1. icann.org/resources/pages/name-collision-2013-12-06-en
2. icann.org/en/groups/ssac/documents/sac-045-en.pdf
3. icann.org/resources/pages/name-collision-2013-12-06-en
4. newgtlds.icann.org/sites/default/files/agreement-approved-02jul13-blackline-16oct13-en.pdf
5. icann.org/resources/pages/name-collision-2013-12-06-en
6. icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf
7. icann.org/resources/pages/name-collision-2013-12-06-en
8. newgtlds.icann.org/sites/default/files/agreement-approved-02jul13-blackline-16oct13-en.pdf
9. icann.org/en/system/files/files/name-collision-framework-30jul14-en.pdf
10. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf
11. icann.org/en/public-comment/proceeding/fourth-proceeding-for-proposed-language-for-draft-sections-of-next-round-agb-14-02-2025
12. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.2
13. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.3
14. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.3-4
15. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.4
16. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.4-5
17. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.5-6
18. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.7
19. itp.cdn.icann.org/en/files/policy-development/topic-29-name-collision-14-02-2025-en.pdf p.2

Get Involved

Interested in Getting More Involved With ICANN and Policy Work?

Consider joining the following groups (as relevant to your business):

- ICANN Business Constituency, icannbc.org
- Intellectual Property Constituency, ipconstituency.org
- Brand Registry Group, brandregistrygroup.org

Upcoming ICANN Meetings

Policy Forum
9 - 12 June, 2025

Annual General Meeting
25 - 30 October, 2025

Community Forum
7 - 12 March, 2026

Markmonitor™

Should you need any further information or assistance, please contact your Domain Portfolio Advisor (DPA) or email customer.service@markmonitor.com

Markmonitor provides strategic domain management solutions that help protect the revenue and reputation of the world's leading brands.

Since 1999, Markmonitor has served the domain portfolio needs of businesses around the globe, including many of the most visited websites in the world. An ICANN accredited domain registrar since its establishment, Markmonitor leverages its extensive industry relationships, innovative technology, and broad expertise to manage and protect company domain portfolios, all with data-driven, white-glove consultation designed to maximize domain portfolio value.