GoDaddy Corporate Domains

Briefing

Beyond Seattle

Key Insights from ICANN82

Developments in gTLD Policy, DNS Abuse,and Registration Data Access

The ICANN82 Community Forum, held in Seattle, WA from March 8–13, 2025, tackled some of the most pressing issues facing the domain name industry today. Key focus areas included preparations for the next round of new gTLDs, efforts to combat DNS abuse, and updates to domain registration data access protocols. As ICANN charts its future direction under new CEO Kurtis Lindqvist, this meeting set the tone for implementation-heavy discussions and global stakeholder engagement.

Next Round of New gTLDs: More Clarity, Higher Stakes

ICANN82 reinforced momentum toward the launch of the next round of new gTLDs, still on track for April 2026. Sessions were held to review the final updates to the Applicant Guidebook (AGB), which will be released in full for an extended public comment period by the end of May 2025. Notable changes from these sessions include clearer language around GAC Early Warnings and more guidance for direct communication between applicants and governments.

Application Fees Finalized

ICANN confirmed the base application fee: $227,000 per gTLD. As covered in that fee includes core evaluations like background screening, financial assessment, and DNS stability review—but not optional services like geographic name support or brand exemption requests. Refunds are now tiered:

- 65% if withdrawn within 10 days of String Confirmation
- 35% after that but before evaluation begins
- 20% if withdrawn pre-contract

RSP Evaluation Program Underway

The Registry Service Provider (RSP) Evaluation Program is moving ahead. All applicants for the next round must now use a pre-approved RSP. As of March, of the 23 RSPs that submitted materials, 6 have been approved. There will be a second RSP window that will run concurrently with the new gTLD application round in April of 2026.

ASP – Uptake Still Modest

The Applicant Support Program (ASP), launched in November 2024, aims to expand global participation in the gTLD space by offering financial and non-financial support. As of March 2025, 18 draft applications were initiated, but only two had been formally submitted. While designed with developing regions in mind, most applications so far are from North America and Asia. Fee discounts range from 75–85%, and auction bid credits of up to 35% are available.

Global Outreach Campaign

ICANN is running a three-phase outreach campaign to promote the next round of new gTLDs to the global market:

- *Phase 1 Brand Revolution* targets corporations and marketers
- *Phase 2 Digital Destination* focuses on city and regional governments
- *Phase 3 Demystifying gTLDs* is tailored to NGOs and under-served communities

These campaigns aim to expand awareness and promote diversity among gTLD applicants.

DNS Abuse: From Accuracy to Contactability

What's the Shift?

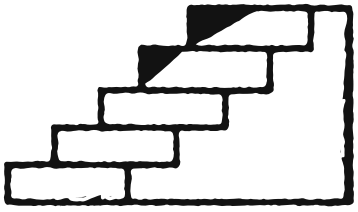
At ICANN82, The topic of registrant data accuracy was broadly discussed. While sessions with the Government Advisory Committee (GAC) were focused on being able to confirm the accuracy and validity of the registrant data representatives from registrars, emphasized that contact ability—not identity verification—is the main requirement from an operational standpoint because knowing that they can reach the registrant is essential for many necessary registrar functions.

Beyond confirming that the contact information for the registrant is functional, identity verification of registrants is not currently critical for most commercial registrars.

Compliance Update: Numbers That Matter

Since the April 2024 DNS abuse-related contract amendments:

- *5,400+* malicious domains mitigated
- *3* registrars received breach notices
- *90%+* mitigation rates (Aug–Nov 2024) per NetBeacon



ICANN is currently conducting a registry audit, and planning an audit on registrars that will incorporate compliance with the new DNS abuse amendments.

Inside the Numbers: What Drives Malicious Domain Registrations?

INFERMAL Report Reveals Key Economic and Technical Incentives Behind DNS Abuse

At ICANN82, a major highlight in the DNS abuse discussion came from the release of a new, in-depth study: the INFERMAL Report (Inferential Analysis of Maliciously Registered Domains). Conducted by KOR Labs in collaboration with ICANN, this research sheds light on the economic and operational features that cybercriminals weigh when registering domain names for phishing attacks.

The study analyzed over 14,000 maliciously registered domains and compared them to a baseline of legitimate domains to pinpoint exactly what makes certain registrar-TLD pairs attractive to bad actors.

Discounts Are a Magnet for Abuse

Here's the headline: every dollar discounted on a domain registration corresponds to a 49% increase in malicious registrations. And if a registrar throws in free web hosting? That spikes phishing registrations by 88%. Conversely, strong registration restrictions were associated with a 63% decrease in malicious activity.

APIs Fuel Automation—and Abuse

Registrars offering public APIs for domain registration saw a 401% increase in abuse volume. Attackers are leveraging these APIs to automate bulk domain purchases, often in conjunction with free services and discounted pricing. This makes it easier than ever to spin up thousands of phishing domains with minimal overhead.

Free Add-Ons Aren't Just Perks—They're Enablers

The presence of free DNS, SSL certificates, email services, and hosting was linked to higher abuse volumes, as they eliminate infrastructure costs for bad actors. While some services (like SSL) benefit both legitimate and malicious users, others—like free hosting—appear to disproportionately enable abuse at scale.

Verification and Restrictions Matter

The most effective deterrents? Proactive registrar restrictions (like identity checks, KYC processes, or limits on domain bundles) and validation of contact information at sign-up. Registrars who verify both email and phone data saw a 70% drop in abuse. Unfortunately, not all registrars implement such checks consistently.

Reactive Enforcement? Helpful, but Not Enough

The report found that takedown speed (i.e., how quickly domains are mitigated after being reported) has only a marginal effect on reducing abuse. Why? Because even a short-lived phishing domain can still capture credentials or inflict harm. This underscores the importance of preventing abuse at the point of registration, rather than relying solely on post-hoc suspension.

Key Takeaway: Service Offerings Matter

The INFERMAL study delivers a clear message to industry stakeholders: how you structure your offerings—pricing, features, access models—matters. Registrars who align their incentives with abuse deterrence (e.g., enforcing upfront verification, limiting automation, reducing unnecessary freebies) are far less likely to be exploited by cybercriminals.

As ICANN and the community continue to grapple with DNS abuse, this data-driven report is a valuable addition to the conversation. Expect it to inform future contractual requirements, policy recommendations, and perhaps even a more formalized response framework across the ecosystem.

Regulatory Spotlight: NIS2 and the Global Compliance Puzzle

EU Member States Begin Transposing NIS2—But Harmonization Remains a Work in Progress

While much of the conversation at ICANN82 focused on DNS abuse and the next round of new gTLDs, a quieter but equally impactful thread emerged: the implementation of the NIS2 Directive across the European Union. As of March 2025, EU Member States are in varying stages of transposing this directive into national law— and registrars are watching closely.

What Is NIS2, and Why Does It Matter?

The NIS2 Directive (short for the EU's "Network and Information Security Directive 2") is an ambitious update to cybersecurity legislation aimed at improving the resilience of essential and digital services—including domain name registries and registrars. Under NIS2, these actors are now classified as essential or important entities, subject to stricter obligations around abuse mitigation, data accuracy, and reporting.

For registrars and registries operating in the EU—or simply serving EU customers—this means new responsibilities. These may include:

- Proactive DNS abuse response protocols
- Contact data validation (pre- or post-registration)
- Maintaining accurate and up-to-date registrant information =
- Mandatory incident reporting within a set time frame

But while the goals of NIS2 are clear, the execution varies wildly. Some Member States have introduced stringent requirements; others have yet to finalize legislation. This patchwork approach is creating uncertainty for domain service providers operating in multiple jurisdictions.

Compliance Templates in Demand

At ICANN82, several registrars expressed a desire for standardized NIS2 compliance templates—a "minimum viable framework" they could adopt across Member States. The idea is to avoid having to navigate 27 slightly different sets of rules and instead promote a unified compliance model, akin to a "best practice baseline" aligned with both NIS2 and ICANN obligations.

Whether such a harmonized model will emerge remains to be seen, but ICANN indicated that it is monitoring national implementations and engaging in bilateral discussions with regulators and contracted parties to encourage consistency.

Bottom Line: NIS2 is forcing registrars, registries, and ICANN itself to rethink what compliance looks like in a fragmented regulatory landscape. For now, flexibility and foresight are key—because the only constant across Member States seems to be change.

RDRS at One Year: Pilot Performance and Policy Crossroads

Request Volume, Legal Hurdles, and the Question of What Comes Next

The Registration Data Request Service (RDRS) pilot has officially marked one year in operation, and ICANN82 offered a prime opportunity for community evaluation. Initially launched in November 2023, the RDRS was developed as a stopgap solution—a lightweight, voluntary platform designed to route requests for non-public registration data to participating registrars.

Now, with 18,248 initial lookups logged as of October 2024, the community is asking a key question: Is RDRS delivering what it promised? Or has it fallen short of its mandate?

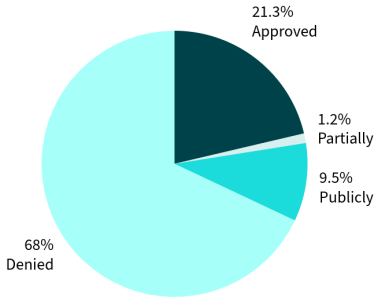
One Year Metrics: Volume and Outcomes

A recent GAC metrics graphic revealed the full request journey:

- ***5,237 lookups*** resulted in immediate success (likely because the data was already public).
- ***10,894 requests*** were blocked at the source—either because the domain fell under a ccTLD, military/ government space, or because the registrar was not participating in the pilot.
- Just ***2,025 formal data requests*** were submitted through the system, meaning that the data was not publicly available.

Of those formal data requests:

- **422 were approved**
- **23 were partially approved**
- **188 revealed the data was already "publicly available"** (likely via proxy contact)
- **1,345 were denied**, with reasons ranging from legal constraints and insufficient information to outright transfer of the domain.



These numbers have sparked a diversity of interpretations across the community.

Volume vs. Value: A Divided Perspective

Some in the community argued that the pilot's numbers are low, due to limited participation in and marketing of the pilot, and should not be used as a proxy for demand. With limited registrar participation and no standardized request format, these numbers are measuring the demand for a system with very limited participation, not for registrant data access itself.

Conversely, others view the early adoption differently - achieving a 10–25% share of request traffic in year one, with minimal promotion, could show a modest success for a pilot tool. This interpretation hinges on the idea that RDRS is complementary to—not a replacement for—existing channels, such as direct abuse reporting and other legal pathways.

Structural Challenges and Lessons Learned

Discussions within the RDRS Standing Committee emphasized several operational and policy friction points:

- ***Lack of Registrar Participation***: Over 4,900 lookups were blocked due to non-participating registrars. Without broader coverage, the system cannot serve as a reliable global interface.
- ***No SLAs or Enforcement***: Without service-level agreements, RDRS response times remain inconsistent. The system also lacks accountability mechanisms for delayed or ignored requests.
- ***Unclear Request Outcomes***: Many rejections were vague or required follow-ups. The system doesn't yet distinguish between "request denied due to legal block" vs. "more information needed."

Bottom Line: RDRS has revealed the growing pains of balancing global access needs with decentralized authority and legal fragmentation. The pilot has yielded important data—but its future depends on whether the ICANN community chooses to scale it, replace it, or let it sunset in favor of a broader access framework.

Looking Ahead

From policy to implementation, ICANN82 reflected a shift toward operational readiness, with a healthy dose of geopolitical awareness. As the next round of gTLDs approaches, and abuse mitigation and data access mechanisms mature, stakeholders should prepare for a high-impact 2025.