ICANN 84 ANNUAL GENERAL MEETING

GAC Meeting with the SSAC

15:00 16:00 UTC

28 October 2025

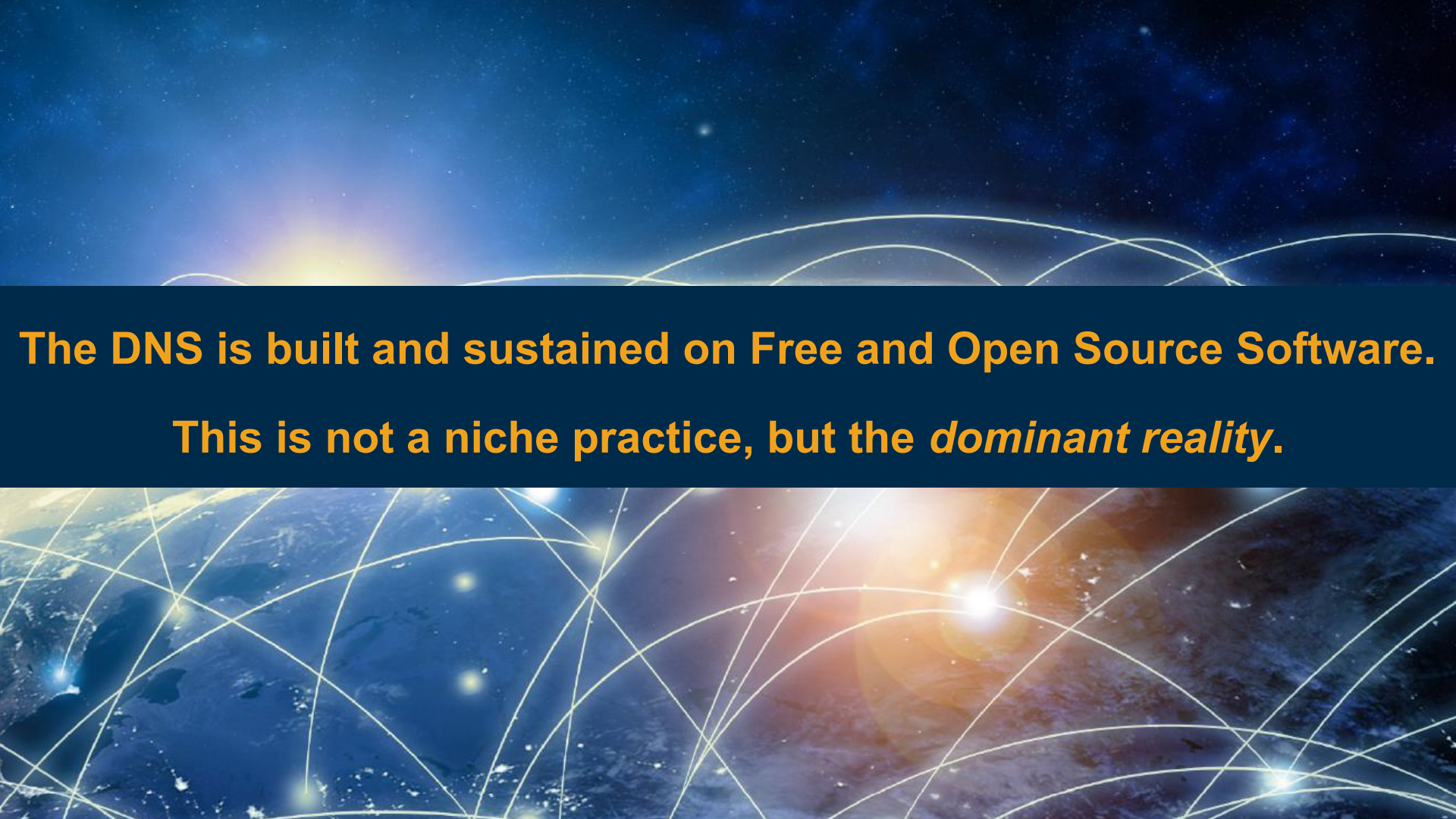
Agenda

1. **Importance of FOSS in the DNS Industry (20 mins)**
   a. SSAC to introduce the recent report on the role of FOSS in DNS
   b. Highlight recommendations regarding public policy to support FOSS, especially in the global DNS ecosystem
2. **Impact of string collision and similarities on security and stability (15 mins)**
   a. Short primer on why this is an issue:
      i. String collisions (similarities) within the public DNS
      ii. String collisions with alternative naming systems and namespaces
   b. Recommendations and safeguards in the next-round that mitigate collision risks
3. **DNS Abuse Policy Issues Paper (10 mins)**
   a. (technical) recommendations and requirements based on the Issues Paper
4. **Possibilities for cooperation between SSAC and GAC (10 mins)**
   a. Opportunities for cooperation in the upcoming GNSO policy track(s) on DNS Abuse?
   b. Involvement of SSAC in ICANN policy track(s) on Urgent Requests?

Overview of SAC132

The Domain Name System Runs on Free and Open Source Software (FOSS)

Maarten Aertsen, SSAC


The DNS is built and sustained on Free and Open Source Software.
This is not a niche practice, but the *dominant reality*.

FOSS: More Than "Free" Software

THE FOUR FREEDOMS

USE

The software for any purpose.

STUDY

How the software works.

SHARE

And redistribute copies.

CHANGE

And release improvements.

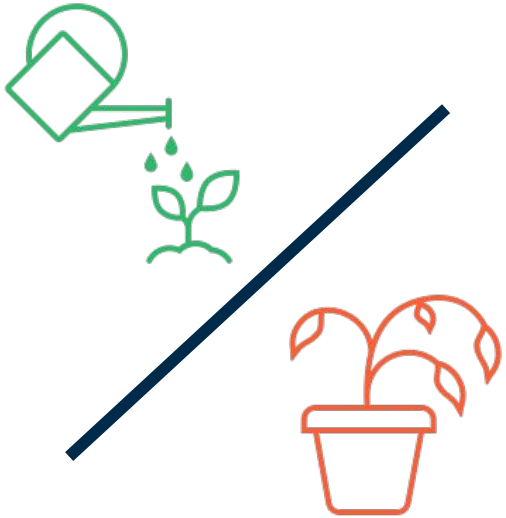
Inherent Risks of FOSS in General

Maintainer Burnout

- Most FOSS relies on single, unpaid volunteers. There is a corresponding risk of burnout and project abandonment.

No Warranty, No Guaranteed Support [by default]

- No entity required to fix problems
- No default Service-Level Agreements
- Operators must take responsibility



Financial Fragility

- Funding decoupled from Use ("Free-rider")
- Small initiatives/orgs are vulnerable to funding shocks resulting from new regulatory burdens.

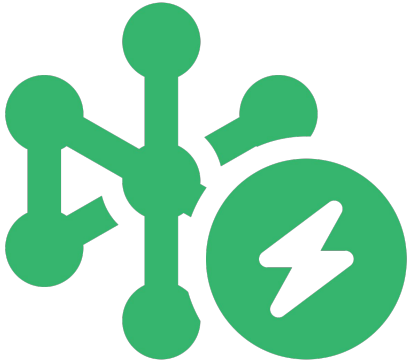
Strengths of FOSS in DNS

Transparency & Collaborative Security

- Academic & operator community maintain a strong, active culture of openly scrutinizing FOSS DNS software.
- Flaws are "openly discussed and fixed at top speed"
- Operators appreciate the ability to diagnose, verify and "expedite patching" of vulnerabilities

Stability of Core DNS Projects

- Most popular DNS projects are supported by long-lived, stable organizations that have been maintaining the software for 20+ years.



Operational Resilience Through Diversity

- Multiple implementations enable diverse software stacks, avoiding single points of failure and preventing vendor lock-in.

Security - Not Better or Worse, but Different

Understanding what truly determines software security

What DOESN'T Determine Security

❌ Open vs. closed source code

❌ Paid vs. volunteer maintenance

❌ Commercial vs. non-profit

What DOES Determine Security

✅ Quality of development process

✅ Code review rigor

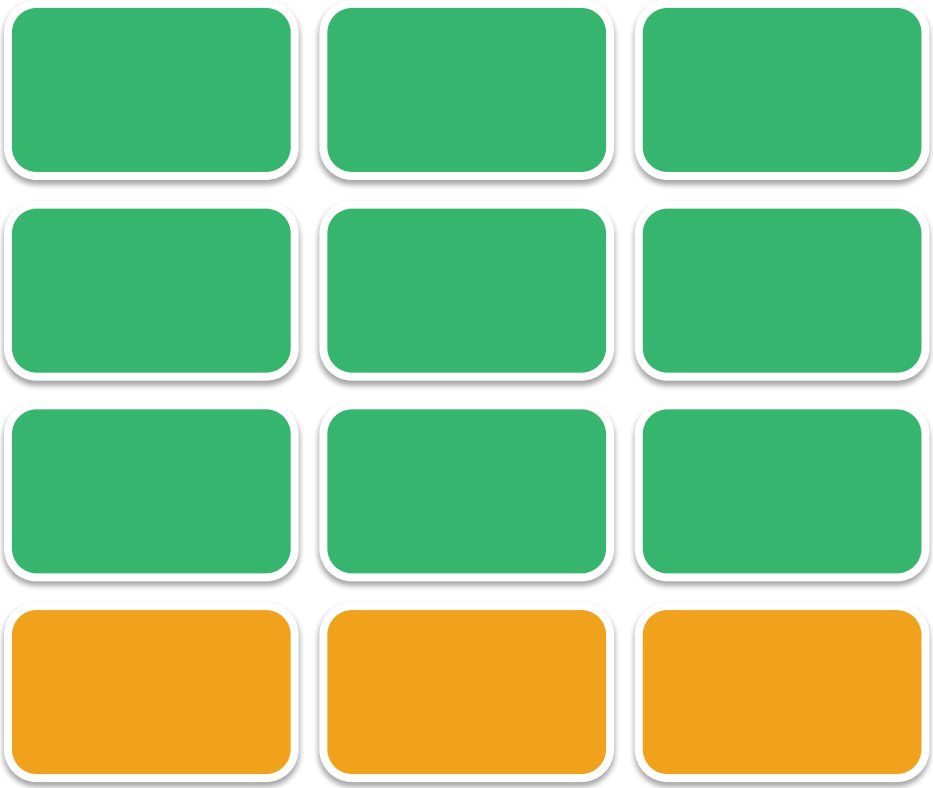
✅ Testing practices

✅ Vulnerability disclosure process

✅ Patching speed

✅ Maintenance sustainability

FOSS in the Root Server System

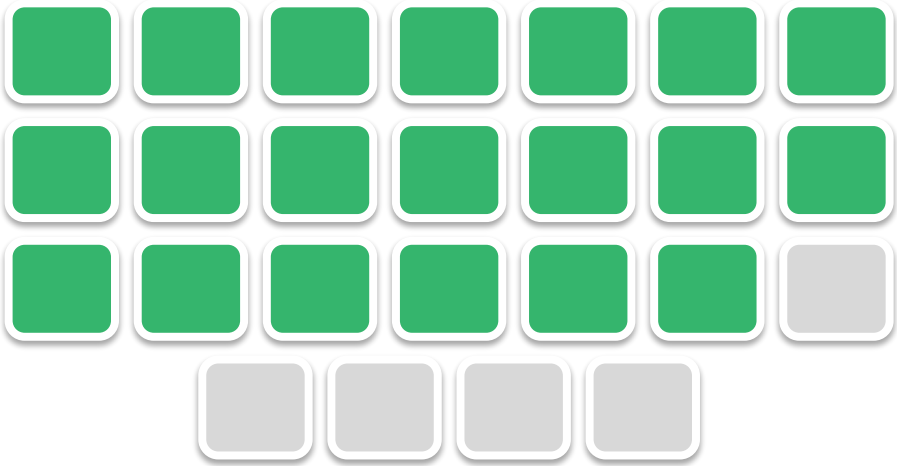


9 / 12 Root Server Operators use FOSS exclusively

TLD Operators

Top TLD Providers
9 / 10

Top ccTLD Providers
20 / 25



FOSS in Registry Systems

Model 1
Entirely FOSS

Viable, complete, end-to-end registry platforms.

Examples:
- FRED
- Nomulus

Model 2
Proprietary on FOSS

Custom, proprietary logic built on a FOSS foundation.

Examples:
- PostgreSQL
- nginx

10 out of 10 major registry platforms we surveyed incorporate FOSS components.

Resolver Infrastructure

FOSS has a ***substantial*** presence across the entire resolver ecosystem, from local networks to global cloud platforms.

Local ISP/Enterprise

- ~80% of users worldwide
- Predominantly FOSS

Cloud Platforms

- At least 4 major hyperscalers rely on FOSS

Public Resolvers

- Quad9 (9.9.9.9)
- DNS4EU
- Cloudflare 1.1.1.1
  - Proprietary core, surrounded by FOSS

FOSS is the foundation of critical DNS infrastructure

≥9/12
Root operators use FOSS exclusively

10/10
Major registries use FOSS components

9/10
Top TLD providers use FOSS

Substantial
FOSS presence across resolver ecosystem

Why Traditional Regulation Backfires on FOSS

Traditional Regulation

Assumes a vendor-customer model with **financial transactions** and **contracts** at every step.

The FOSS Reality

- No guaranteed vendor, contract, or payment.
- **DNS operators—not FOSS maintainers—**must take responsibility for the FOSS implementations they deploy,

The Unintended Burden

Compliance costs and **legal risks** are imposed on FOSS maintainers who have no ability to absorb them.

The Backfire

- Maintainers **abandon projects**, switch to proprietary licenses, or avoid the region.
- The software we depend on becomes **less secure** and **less available**.

Contemporary Approaches to FOSS Regulation

Key strategies from recent global regulatory frameworks

Allocate Responsibility Appropriately

2023 US CYBERSECURITY STRATEGY · 2025 UK CODE

Put obligations on commercial integrators & deployers, not maintainers.

Incentivize Sustainable Maintenance

EU CYBER RESILIENCE ACT

Introduce optional 'steward' role to incentivize community support and maintenance for critical project.

Adapt Supply Chain Concepts

EU NIS 2 IMPLEMENTING ACT

Recognize that no contracts means no direct supplier relationship, adapt regulatory strategy accordingly.

Avoid Conflicting Regional Regimes

EU NIS 2 DIRECTIVE

Prevent regulatory overlaps for globally critical infrastructure like root servers

Five Actionable Guidelines for Policymakers

1. Acknowledge the Critical Role of FOSS
2. Consult the FOSS Community
3. Make Use of Contemporary Cases
4. Incentivize FOSS Sustainability
5. Address Systemic Risks Collectively

Impact of String Collisions on Security & Stability

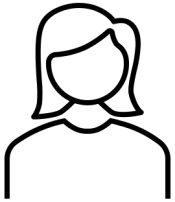
Former chair of NCAP Study Two,
Suzanne Woolf
Chair for SSAC RIDE Work Party,
Rick Wilhelm

What Is A Name Collision?

Think of domain names like house addresses.

If two houses share the same address, it becomes hard to know which one mail or deliveries should go to. There are also security issues if the mail gets delivered to the wrong address.

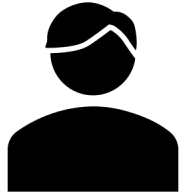
In the DNS, name collisions occur when a domain used in the global DNS namespace is also used in a different namespace (e.g., private enterprise), where users, software, or other functions may misinterpret it.



Home of Danielle EndUser

123 Home Ave
Example, ST USA 12345

The impact of name collisions is much greater than this metaphor might suggest.



Home of Steve Networks

123 Home Ave
Example, ST USA 12345

What Is NOT A Name Collision?

Name Collision

- ➜ A technical problem causing security & stability issues.
- ➜ Caused by delegating the exact same TLD already used in private networks.
- ➜ example.corp (Private Network Use)
  example.corp (Public Domain)
- ➜ ***Risk:*** Queries for private names "leak" to the public DNS, causing technical conflicts and security failures.

String Similarity

- ➜ A user problem causing confusability issues.
- ➜ Caused by different public TLDs that look or sound alike.
- ➜ .example (lowercase '`l`')
  .example (uppercase '`I`')
- ➜ ***Risk:*** Enables phishing, fraud, and loss of user trust.

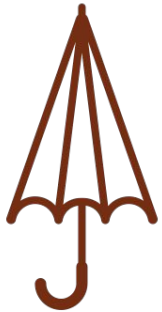
Understanding Name Collisions is Important for Internet Security

- **Risk of unintended consequences**. Businesses have used labels as internal TLDs in private namespaces that may leak to the global internet.
- **Introduction of new gTLDs increases probability of name collisions.** A larger pool of potential names increases the possibility that a gTLD string might unintentionally overlap with names already used in private networks or internal naming systems.
- **Measuring name collisions is difficult due to evolution of technology and network infrastructure**. Privacy enhancements in the DNS and alternative naming systems have made the DNS landscape more complex and measurements more difficult.

The Evolution of Name Collision Analysis

- 2012 new gTLD round accelerated growth of the root zone, prompting questions about what happens when new strings are added that may already be in use
- 2013: SSAC issued SAC062, highlighting that significant security and stability problems may occur as a result of name collisions
- The most significant detected string collisions were .home, .corp, and .mail, which the Board suspended indefinitely
- 2017: ICANN Board tasked SSAC to conduct comprehensive studies to enable all future gTLD delegations to be done in a ***secure, stable, and predictable manner***

Name Collision Risk Assessment Framework



Goal 1: Ensure that name collisions can be assessed

- Root zone delegation is required for empirical analysis of potential name collisions
- Requires ability to define, collect, and analyze relevant measurements (see Study 2 Report)

Goal 2: Provide a process for ICANN to evaluate mitigation and remediation plans for identified name collisions

- While known causes may inform mitigation and remediation plans, further investigation may be required for specific labels
- Ensures that a mitigation or remediation plan (or both) can be developed and assessed

Name Collision Risk Assessment Process

- Applicants perform proactive assessment using public data.

- A Technical Review Team (TRT) assesses initial risk.
- "High risk" strings require a mitigation plan review.

- Temporary delegation occurs for live data assessment.

- TRT provides a final risk recommendation to the ICANN Board
- TLD applicant may propose risk mitigation plan for TRT review
- ICANN Board makes the final delegation decision

Benefits of Name Collision Risk Assessment Framework

The Name Collision Risk Assessment Framework provides the following benefits:

- **Proactive Risk Management:** Identifies name collision risks and allows for the development and review of mitigation strategies *before* they cause harm.
- **Consistent & Effective:** Centralized approach ensures thorough risk assessment and mitigation across all new gTLD applications.
- **Data-Driven:** Enables informed decisions for secure expansion of the Internet's namespace.
- **Privacy Concerns Addressed:** While risk is inherent in assessing name collisions, the privacy risk of *not* accurately assessing name collisions is greater than the risk associated with assessment. Early risk detection and informed mitigation are crucial for the security and stability of the DNS.

What About Blockchain & Alternative Naming Systems?

SSAC Work Party Focused on Keeping the DNS Safe as Technology Evolves

🎯 OUR GOAL

Develop clear guidelines to enable new technologies like blockchain and Web3 integrate responsibly with the DNS while protecting security, stability, and user trust.

📚 KEY AREAS OF STUDY

🔄 Domain Lifecycle

Managing synchronization when domains expire or transfer while still linked to new services.

😵‍💫 User Confusion

Preventing fraud when similar names exist in DNS and new systems.

🔐 Security & Stability

Analyzing potential risks that could be introduced to the DNS.

DNS Abuse Policy Issues Paper

Open Discussion between GAC-SSAC:

- Recommendations and requirements based on the Issues Paper

Possibilities for cooperation between SSAC and GAC

Open Discussion between GAC-SSAC:

- Opportunities for cooperation in the upcoming GNSO policy track(s) on DNS Abuse?
- Involvement of SSAC in ICANN policy track(s) on Urgent Requests?

Thank you