KINDNS

KINDNS:

A framework to improve the security and resilience of the DNS

Yazid AKANHO
Technical Engagement Manager - MEA
ICANN


KINDNS
KINDNS
KINDNS
ICANN
Follow us on Twitter:
@4KINDNS

How kind is your DNS to the Internet ?

KINDNS

- *DNS translates human-readable names into IP addresses.*
- *A **critical function** for the Internet and its services (emails, web, cloud services, online payments and services, etc.)*
- ***Contributes to the security and performance of the Internet**: distributed functions, caching, DNSSEC, other security mechanisms.*
- ***DNS incidents** can impact organizations: reputation, productivity, service disruption, data breaches, etc.*
    - *DNS as attack vector, DNS misconfiguration or vulnerabilities.*
    - *Low/moderate/severe/critical/local/large, difficult to measure impacts.*

What is KINDNS ?

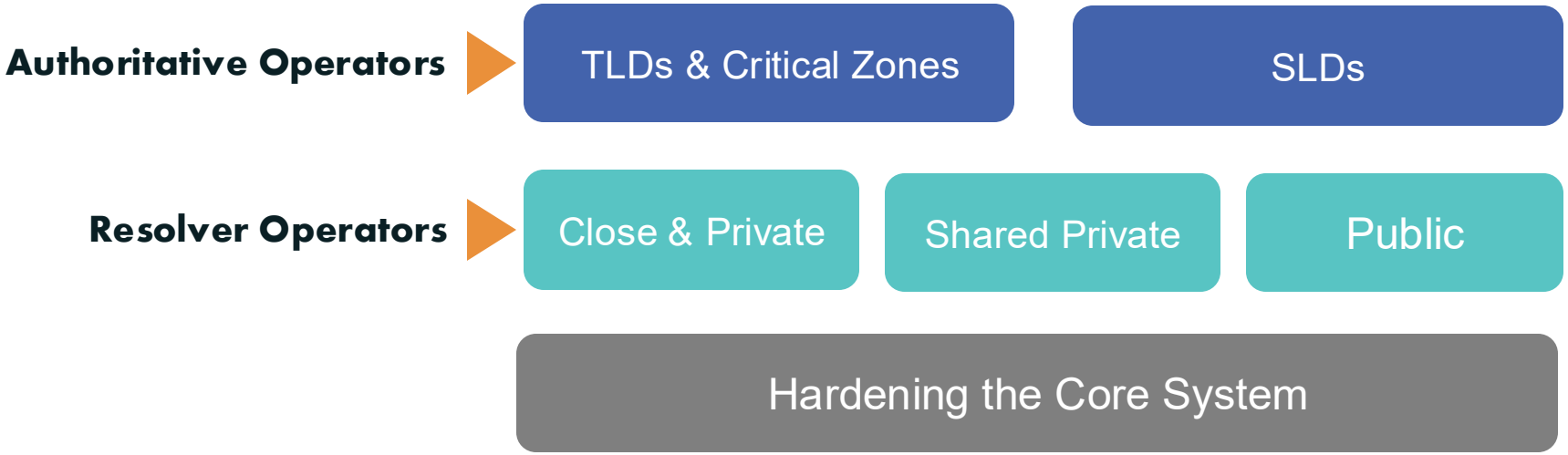
KINDNS

Knowledge-sharing and **I**nstantiating **N**orms for **D**NS
(Domain Name System) and **N**aming **S**ecurity

*A simple **framework** that can **help a wide variety of DNS operators**, from small to large, to follow both the **evolution of the DNS** protocol and the best practices that the industry identifies for better security and more effective DNS operations.*

*….. is pronounced "**kindness**"*

Target Operators



Each category has 6-8 practices that we encourage operators to implement.
See www.kindns.org, for more details.

Authoritative DNS Operators of Critical Zones

KINDNS

TLDs & Critical Zones

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Authoritative DNS Operators of SLDs

KINDNS

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Closed & Private Resolver Operators

KINDNS

*Private resolvers are **not publicly accessible** and cannot be reached over the open internet. They are typically found in corporate networks or other restricted-access networks*

Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled
2. Access control list (ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. Authoritative servers for a given zone **MUST** run from a diversified Infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Shared Private Resolver Operators

Shared private resolver operators are typically ISPs or similar hosting service providers. They offer DNS resolution services to their customers (mobile, cable/DSL/fiber users, as well as hosted servers and applications).

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. For privacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Hardening the Core

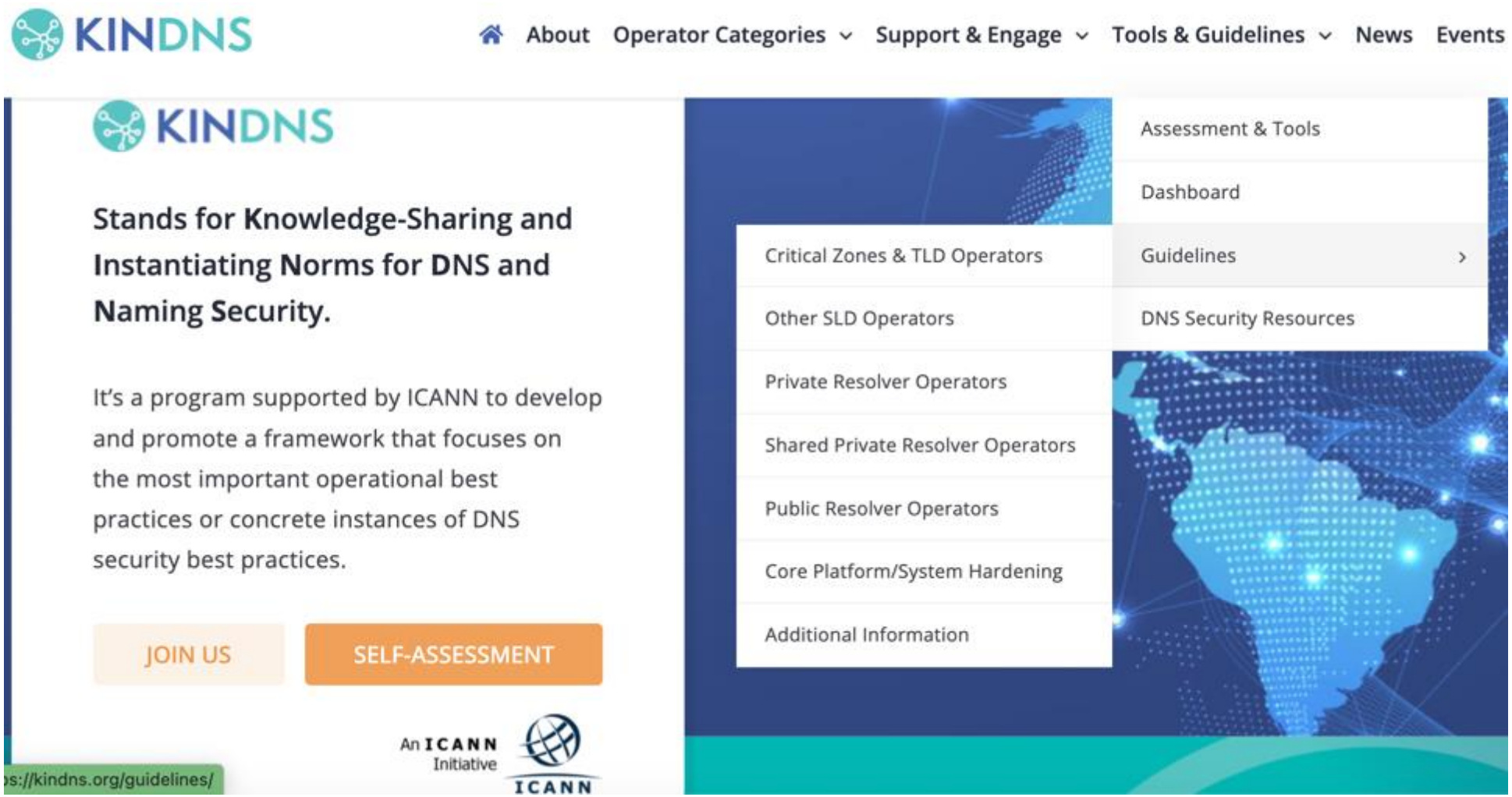
KINDNS

In addition to implementing best practices for DNS security and for DNS availability and resilience, all operators must pay ***careful attention to practices for hardening the platforms*** *their DNS services use.*

Core Hardening

1. ACLs **MUST** be implemented to control network traffic to your DNS servers
2. BCP38/MANRS egress filtering **MUST** be implemented
3. The configuration of each DNS server **MUST** be locked down
4. User permissions and application access to system resources **MUST** be limited
5. System and service configuration files **MUST** be versioned
6. Access to management services **MUST** be restricted
7. Access to the system console **MUST** be secured using cryptographic keys and/or two factor authentication mechanism.
8. Credentials Management for customer access **MUST** adhere to best practices

Practices are documented



Self-assessment & Enrollment

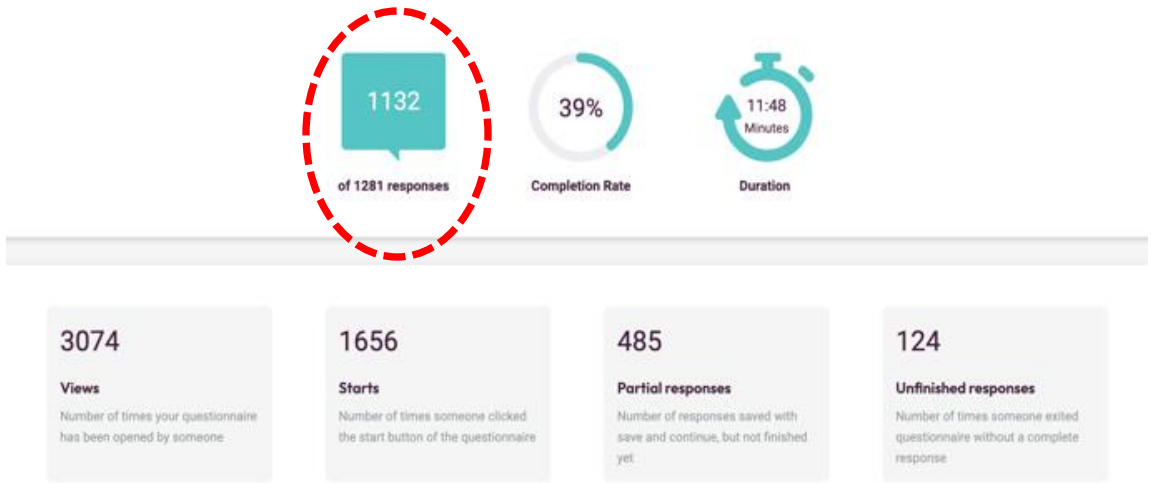
1. Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices.

   - self-assessment is **anonymous**
   - **reports** can be downloaded directly from the web site.

2. Operators can enroll as participant to one or many categories covered by KINDNS.

   - Participation in the KINDNS initiative means voluntarily committing to implement/adhere to agreed practices.
   - Participants become goodwill ambassadors and promote best practices.

Some statistics (Aug 2025)



- First Response 05 Aug 2022 02:07 pm
- Last Response 07 Aug 2025 08:28 am

Number of responses	Average Duration	Completion rate
2272	08 min 26 sec	40%

Critical zone & TLD Operators: 8

Other SLDs Operators: 4

Share Private Resolvers: 12

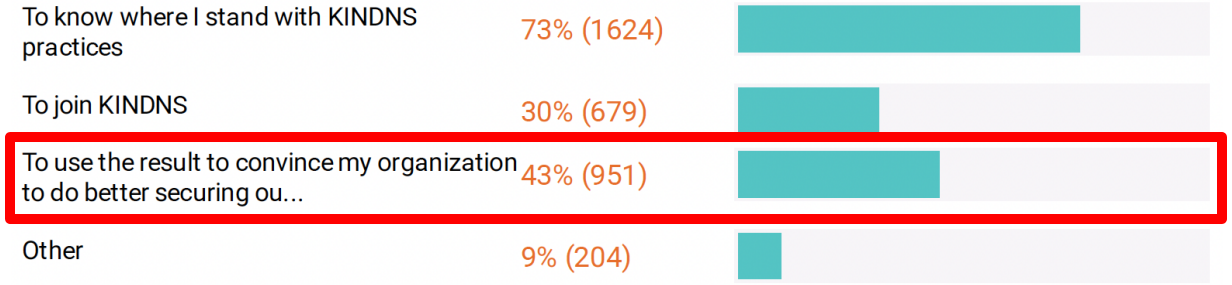
Private Resolver Operator: 4

Public Resolver Operator: 1

High uptake for Self-assessment

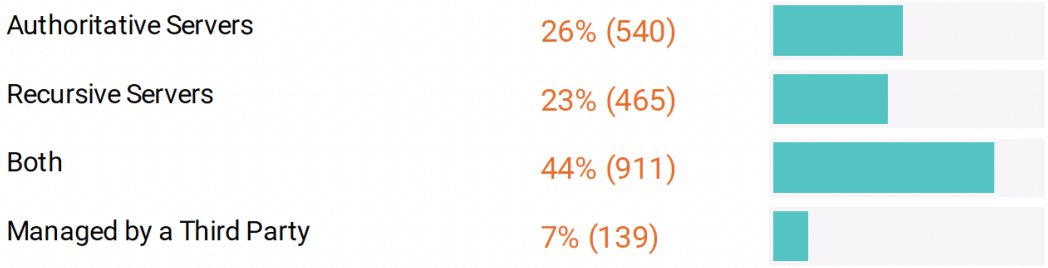
Some statistics (Aug 2025)

1. Why are you taking this self-assessment?



2. Part 1 Core DNS Operation Practices Assessment

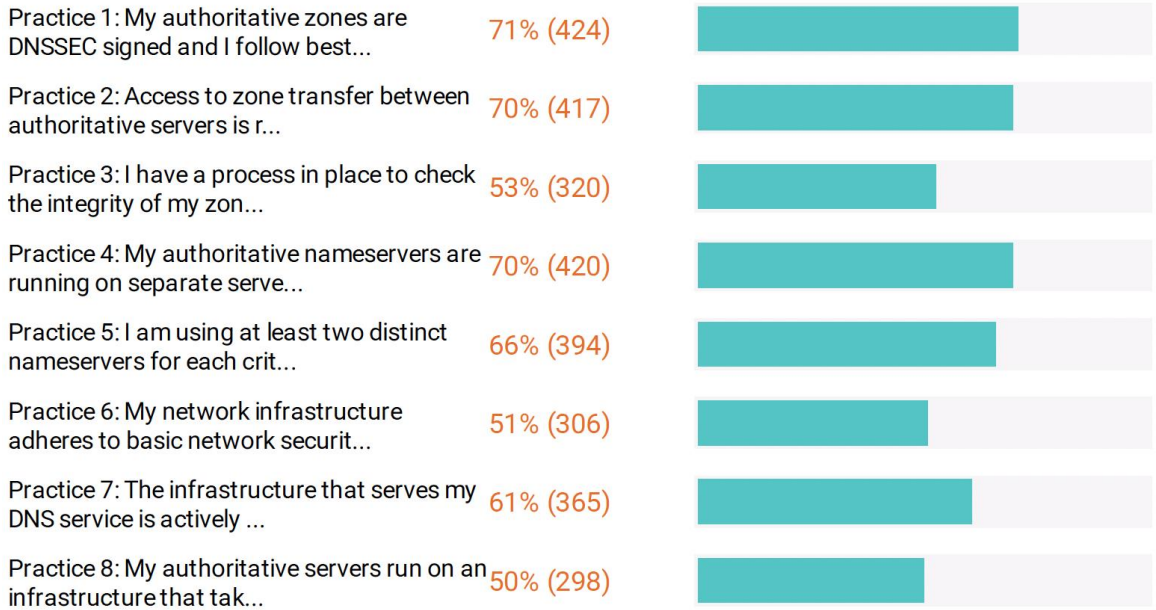
Which component(s) of the DNS do you run?



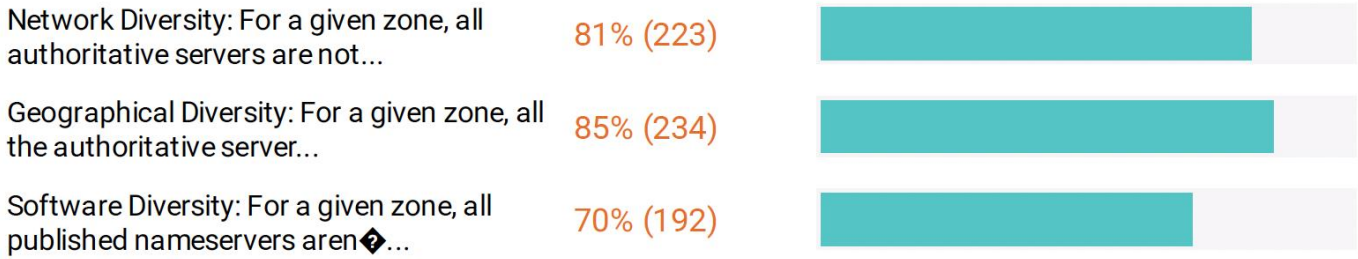
3. What Type of Authoritative Zone Do You Manage?

Type(s) of authoritative zone that you manage

4. As Authoritative Nameserver manager for one or more TLDs or Critical Zones, I implement and adhere to the following practices:



5. Can you tell us more about your operational diversity practices?



Some statistics (Aug 2025)

KINDNS

7. What type of Recursive Resolver do you run?

Type of recursive resolvers you run

Private Recursive Resolvers	55% (593)
Shared Private Recursive Resolvers	25% (269)
Public Recursive Resolvers	20% (210)

8. As a Private Recursive Resolver operator, I implement and adhere to the following practices:

Practice 1: I have DNSSEC validation turned on for my resolvers	69% (376)
Practice 2: I use ACLs to restrict who may send recursive queries to m...	76% (412)
Practice 3: I have QNAME minimization turned on for my resolvers	43% (233)
Practice 4: My resolvers don't run on the same server as any authori...	70% (382)
Practice 5: I have at least one alternate resolver I can point my user...	70% (379)
Practice 6: The infrastructure that serves my DNS services is actively...	72% (393)

12. Do you have proper credential management practices and processes implemented?

Yes	87% (383)
No	13% (59)

15. Network Security: These best practices are aimed at preventing unauthorized network access to your DNS servers and ensuring your internal traffic does not leak onto other networks. Please select the statements that match your operational practices.

Practice 1: ACLs are implemented to restrict network traffic to your D...	93% (792)
Practice 2: BCP38/MANRS egress filtering is implemented so that no net...	60% (517)

17. Customer-Facing Portal: These best practices aim at supporting the security hygiene of accessing your customer portal. You should pay particular attention to robust credential management practices for your customer-facing portal. Please select the statements that match your operational practices.

Practice 8: Credentials for customer access (Registrants and other DNS...	61% (381)
Practice 9: I have an internal policy in place to avoid the use of wea...	86% (542)

Selecting BCPs

How do we identify them ?

- Draw from own operational experience
- Ask operators (NOG lists, communities)
- Review RFCs and other standards
  https://powerdns.org/dns-camel/
- Shortlist based on relevance, ease of implementation, and how widespread the adoption is

Ask operators to review the selection (kindns-discuss)

Debate and justify choices

Engaging the community

KINDNS

Operators must agree on the selected BCPs

kindns-discuss list launched in 2021

- Encouraged operators from all backgrounds to join
- When in doubt, we asked community for advice on what they consider to be a BCP or not
- Some things were debated – is DNSSEC validation a **MUST** nowadays ? (We think so ☺)
- Some practices weren't implemented widely enough, or too complicated (not low hanging fruit) for small operators
  - e.g. Anycast

Current Focus: Phase 2

Service Platform Hardening

Front-end

- Re-Activate the full enrollment form
- Translate the website and the tools into other languages
- Evolve the Self-assessment to technically measure/assess practices implementation.
  - Two views: Internal & External
  - measure implementation by collecting anonymized data from the self-assessment tool.
  - Integrate a Zonemaster version for Authoritative servers

Back-end

- Integrate the KINDNS server to ICANN E&I monitoring service
- Implement a ticketing system to better track interactions with the public.
- Improve the security fence around WordPress
- Deploy an integrated enrollment management tool (a WP plugin)
- Renew ICANN infosec assessment.
- Directly link self-assessment to enrollment
- Develop an integrated tool to simplify/automate Operator compliance assessment

Current Focus: Phase 2 (con't)

KINDNS

Community Engagement

Community engagement - continue to encourage operators to get onboard to contribute and support the framework:

- Direct 1:1 Engagements
- Convince/Encourage more DNS operators to join
- Workshops & webinars to raise awareness on KINDNS practices as part of our overall DNS ecosystem security awareness program.
- DNSAthons around secure DNS operations
- Develop partnerships with programs such as MANRS and Pulse, internet.nl, etc.

Communication: a more active communication plan to further promote KINDNS

- Publish a series of DNS best practices dedicated blogs
- Develop toolkits to help operators engage with internal decision-makers.

KINDNS v.2 - Discussion Points

1. **Adding Response Rate Limiting (RRL)** to Authoritative Servers' practice
   - ccTLD and critical Zone Operators
   - Other SLDs too?
2. **Addressing 'Split' responsibilities** for Authoritative servers' operation:
   - Zone file content is controlled by a third party. i.e root server operators and the root zone itself.
3. **Access reliability:** Reachability over IPv6, RPKI for the prefix used for the DNS servers.
4. **Community review team**: volunteers from the community to work with staff to help with assessing participating candidates or other aspect of KINDNS practice evolution.
5. **Metrics**: help measure the impact of KINDNS adoption on global DNS operations

Some external additional tools

KINDNS

1. **Zonemaster**: https://zonemaster.net/

   A program that tests a DNS zone configuration with different sanity checks configured in an engine and provides a zone health report.

2. **DNSviz**: https://dnsviz.net/

   Provides a visual analysis of the DNSSEC authentication chain for a domain name, its resolution path in the DNS namespace and lists configuration errors it detected.

3. **SuperTool**: https://mxtoolbox.com/SuperTool.aspx

   An integrated tool that can perform several kind of diagnostics on a domain name, IP address or host name. Documentation available at https://mxtoolbox.com/restapi.aspx

4. **Intodns**: https://intodns.com/

   Checks the health and configuration and provides DNS report and mail servers report.

   … and many others.

Stay Informed and Contribute

Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Mailing list	kindns-discuss@icann.org https://mm.icann.org/mailman/listinfo/kindns-discuss

Assess your DNS infrastructure now

KINDNS

Run the KINDNS assessment for your DNS infrastructure:

https://kindns.org/self-assessment/

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: kindns-info@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg