# KINDNS

Knowledge-Sharing and Instantiating Norms
for DNS and Naming Security

*Strengthening the DNS Ecosystem Through Voluntary Best Practices*

An ICANN Initiative


ICANN


iana

# Why KINDNS Exists

The Domain Name System is critical infrastructure. Every connection on the Internet begins with a DNS query. Yet the operational security of DNS infrastructure varies enormously across the global ecosystem.

### Inconsistent Practices

Large operators implement security measures that suit their business needs. Small operators often lack the resources to keep pace with evolving best practices.

### Capability Gaps

Many organizations that operate DNS infrastructure do not have dedicated DNS security expertise. Basic protective measures go unimplemented.

### No Common Baseline

Until KINDNS, there was no agreed-upon, simple reference that defined what adequate DNS operational security looks like for different types of operators.

# What KINDNS Is

KINDNS is an ICANN initiative that identifies the most important DNS operational security practices and organizes them into a simple, voluntary framework. It is a set of practices that the technical community has agreed represent an adequate baseline for responsible DNS operations.

### Voluntary

Operators voluntarily commit because the practices make their operations more secure and resilient.

### Tailored by Operator Type

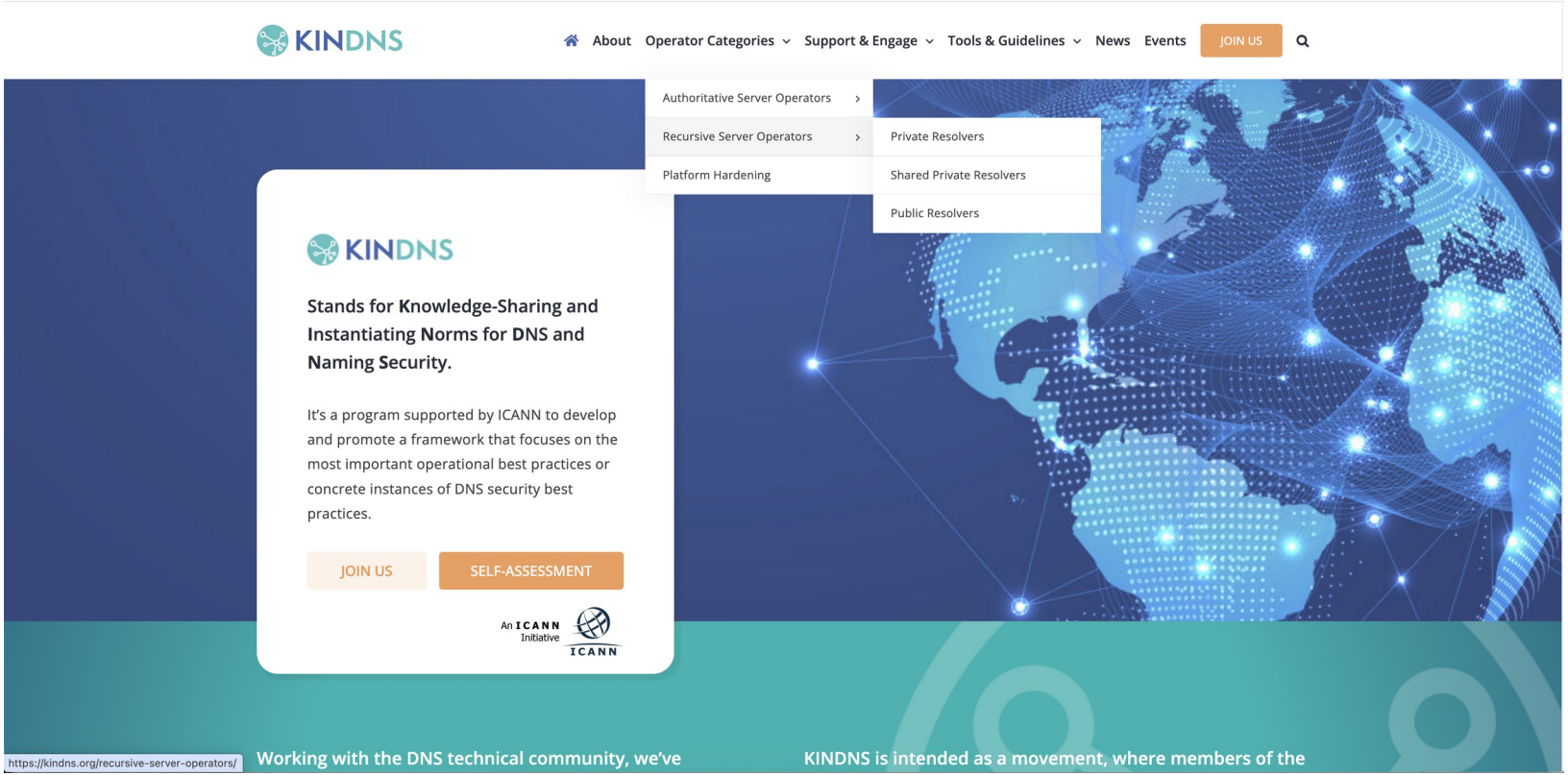
Different practices for TLD operators, second-level domain operators, ISP resolvers, private resolvers, and public resolvers.

### Concrete and Actionable

Each practice comes with implementation guidelines for common DNS software: BIND, Unbound, PowerDNS, and Knot.

### Complementary to MANRS

MANRS addresses routing security (BGP). KINDNS addresses DNS security. Together they cover the two most critical protocol layers.


KINDNS
About
Operator Categories
Support & Engage
Tools & Guidelines
News
Events
JOIN US
Authoritative Server Operators
Recursive Server Operators
Platform Hardening
Private Resolvers
Shared Private Resolvers
Public Resolvers
KINDNS
Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.
It's a program supported by ICANN to develop and promote a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.
JOIN US
SELF-ASSESSMENT
An ICANN Initiative
ICANN
https://kindns.org/recursive-server-operators/
Working with the DNS technical community, we've
KINDNS is intended as a movement, where members of the

# Who KINDNS Is For

KINDNS organizes DNS operators into five categories, each with its own tailored set of practices.

## Authoritative Server Operators

### TLDs & Critical Zones

Registry operators and a few infrastructural zones

### Other SLD Zones

All other second-level domain zones, which is most organizations that host their own DNS

## Recursive Server Operators

### Private Resolvers

Corporate and restricted-access networks. Not reachable from the open Internet.

### Shared Private Resolvers (ISPs)

Internet Service Providers offering DNS resolution to their subscribers

### Public Resolvers

Open services (e.g. 1.1.1.1, 8.8.8.8) and commercial DNS filtering services

*All categories also include Platform Hardening practices covering network security, host security, and credential management.*

# The Practices: ISP Resolvers

ISPs operate recursive resolvers on behalf of their subscribers. When a customer types a website address, the ISP's resolver translates it into an IP address. These resolvers handle (b|m)illions of queries per day and are critical infrastructure for every user on the network.

1. **DNSSEC Validation**
   Confirms that DNS answers have not been tampered with in transit. Without validation, users can be silently redirected to fraudulent websites.

2. **Encrypted DNS Transport (DoH / DoT)**
   Protects DNS queries from eavesdropping. Without encryption, anyone on the network path can see every website a user visits.

3. **QNAME Minimization**
   Limits the information shared with upstream DNS servers during resolution. Reduces unnecessary exposure of user browsing behavior.

4. **Separate Authoritative and Recursive Services**
   Mixing both functions on one server increases the attack surface and the blast radius of a compromise.

# ISP Practices (continued)

5

### Limit Data Retention of DNS Query Logs

DNS query logs are a detailed record of user activity. Retaining them longer than necessary creates privacy risk and a valuable target for attackers.

6

### Resilience Through Diversity

Operate at least two resolvers with geographic and topological diversity. If one fails, service continues. This is basic availability engineering.

7

### Monitor DNS Infrastructure

You cannot secure what you do not observe. Monitoring detects anomalies, service degradation, and potential attacks before they affect users.

### Platform Hardening (applies to all categories)

In addition to the DNS-specific practices above, KINDNS includes platform hardening requirements: network access controls and anti-spoofing (BCP 38/84), locked-down host configurations with only DNS software running, full logging enabled, and credential management with two-factor authentication for customer-facing portals.

# A Deliberately Lightweight Program

KINDNS was designed to be as easy to engage with as possible. The goal is to give operators a clear and approachable path to better DNS security.

### One Simple Website

Everything an operator needs is at kindns.org. Practices, implementation guidelines, self-assessment, and enrollment. No logins, no fees.

### Self-Assessment in 15 Minutes

A straightforward questionnaire walks operators through each practice for their category. It takes 10 to 15 minutes. No data is stored by ICANN. The operator receives a downloadable report of their current posture.

### A Tool for Internal Advocacy

The most common use of KINDNS so far: DNS engineers take the self-assessment report to their managers to show where the organization falls short. KINDNS gives engineers a credible, externally-validated framework to justify the time and budget needed to close gaps.

# Why This Matters for Policymakers

### Voluntary frameworks reduce the pressure for regulation

When industry demonstrates that it can define and adopt meaningful security baselines on its own, the case for prescriptive regulation is weaker. KINDNS provides evidence that the technical community is taking responsibility.

### The practices are grounded in open standards

KINDNS practices are drawn from IETF RFCs, existing BCPs, and operational experience. They represent consensus technical judgment from open standards and operational communities. They are not proprietary or vendor-specific.

### The program scales from small operators to large

KINDNS is designed so that a small ISP in a developing economy and a large registry operator face the same framework, adjusted for their operational role. This universality makes it useful as a reference point for national and regional policy discussions.

### It complements other ecosystem security efforts

KINDNS for DNS. MANRS for routing. These voluntary, community-driven initiatives cover the two most vulnerable protocol layers of the Internet. Policymakers benefit from understanding and supporting both.

# Becoming a KINDNS Ambassador

KINDNS is designed as a movement. Its effectiveness depends on the community itself.

### Join as an implementing operator

Assess your DNS operations against the KINDNS practices for your category. Implement the practices you are not yet following. Enroll at kindns.org to publicly signal your commitment.

### Promote KINDNS to colleagues and peers

Mention KINDNS at NOG meetings, in technical forums, and in conversations with other operators. The more operators who know about the framework, the broader the baseline becomes.

### Use KINDNS in policy discussions

When governments or regulators ask what the Internet technical community is doing about DNS security, KINDNS is part of the answer. It demonstrates that the operational community is capable of defining and adopting its own security norms.

# QUESTIONS?

kindns.org

An ICANN Initiative