Promoting DNS Operational Best Practices

MMNOG5 – 14 January 2023

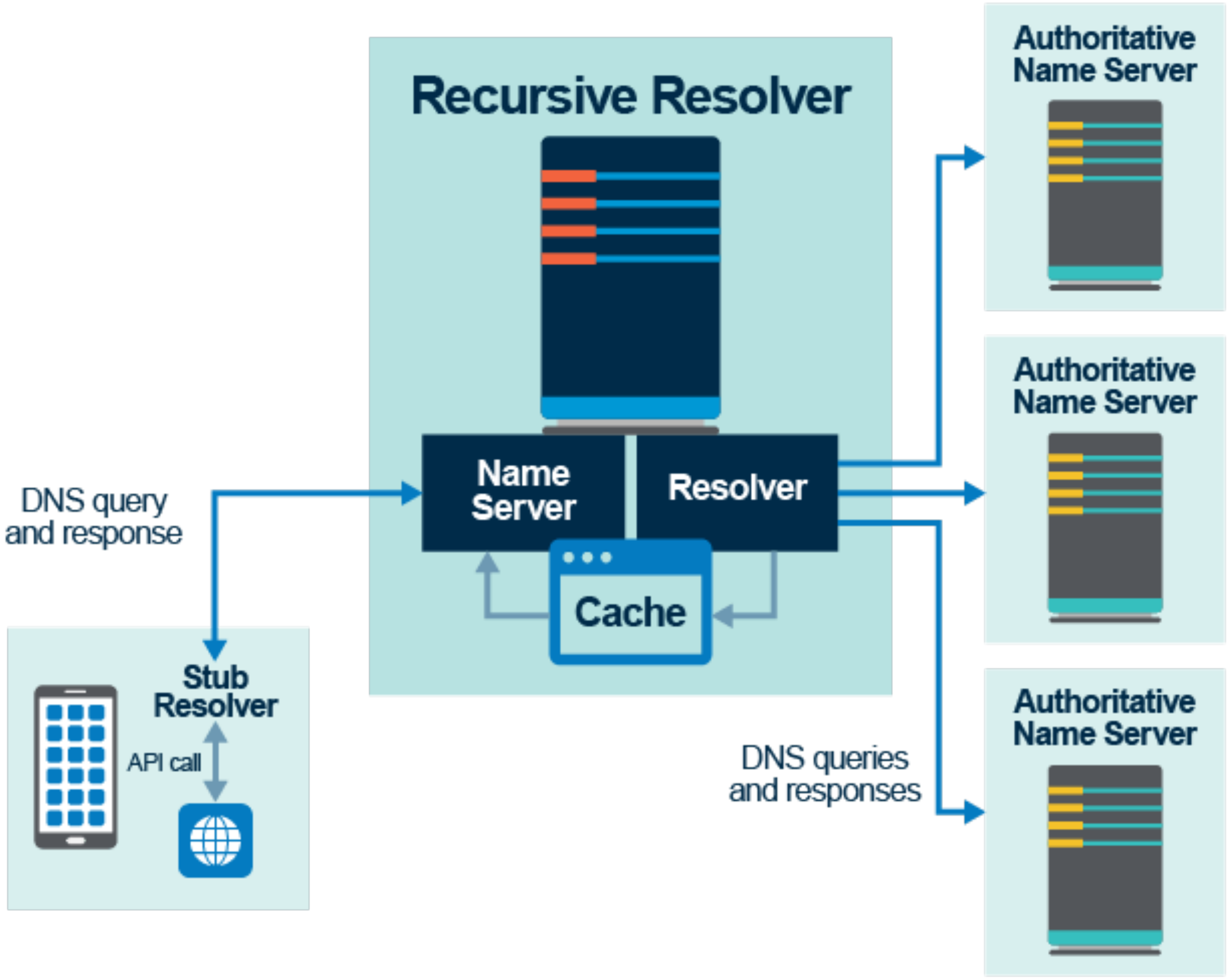
Champika Wijayatunga
Regional Technical Engagement Manager (APAC)

ICANN

DNS contains a wealth of data about your systems

- Your organization’s domain names – **xyz.mm**
- Your organization’s individual host names – **host.xyz.mm**
- IP addresses
- Mail server data (MX records) – **mail.xyz.mm**
- Database locations – **db0.xyz.mm**
- etc

DNS Components at a Glance


Recursive Resolver
Name Server
Resolver
Cache
DNS query and response
Stub Resolver
API call
DNS queries and responses
Authoritative Name Server
Authoritative Name Server
Authoritative Name Server

Root Server

.

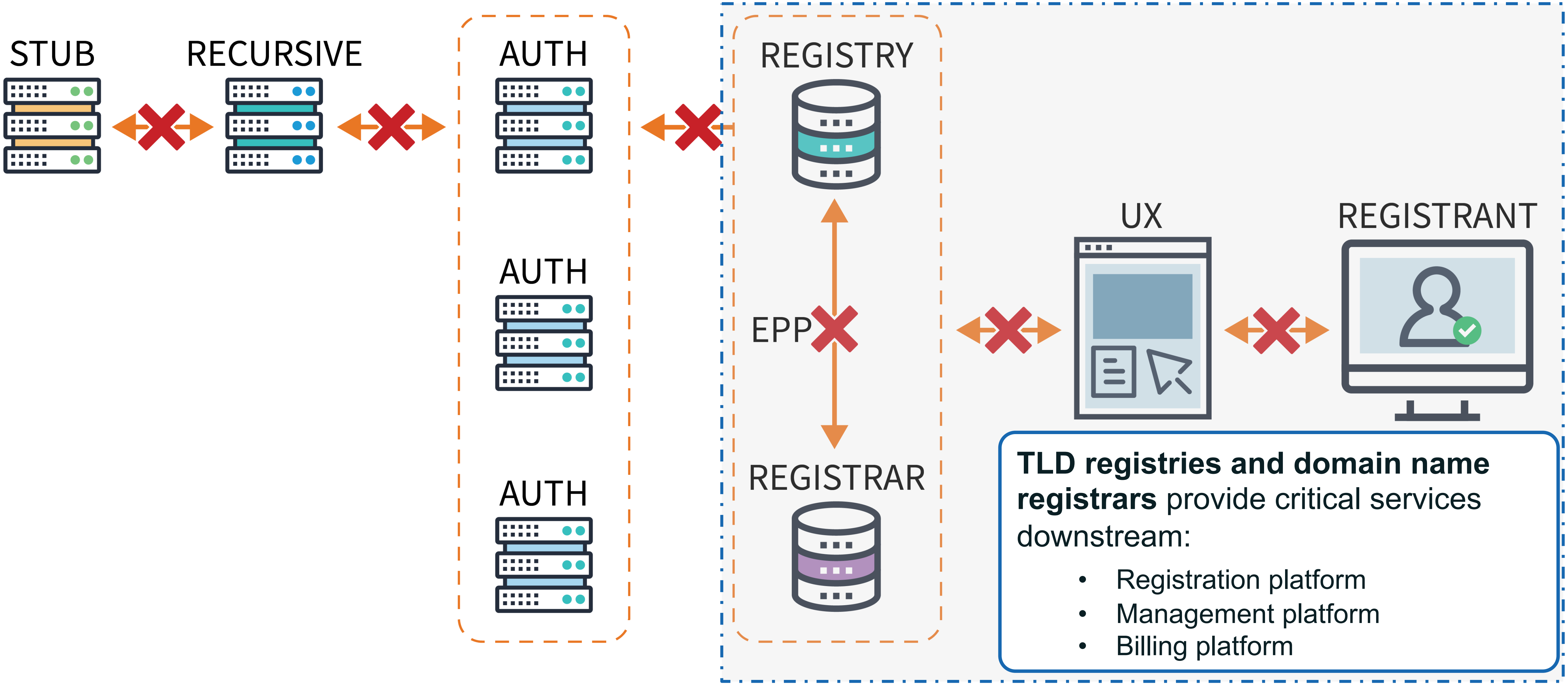
TLD Server

mm.

SLD Server

example.mm.

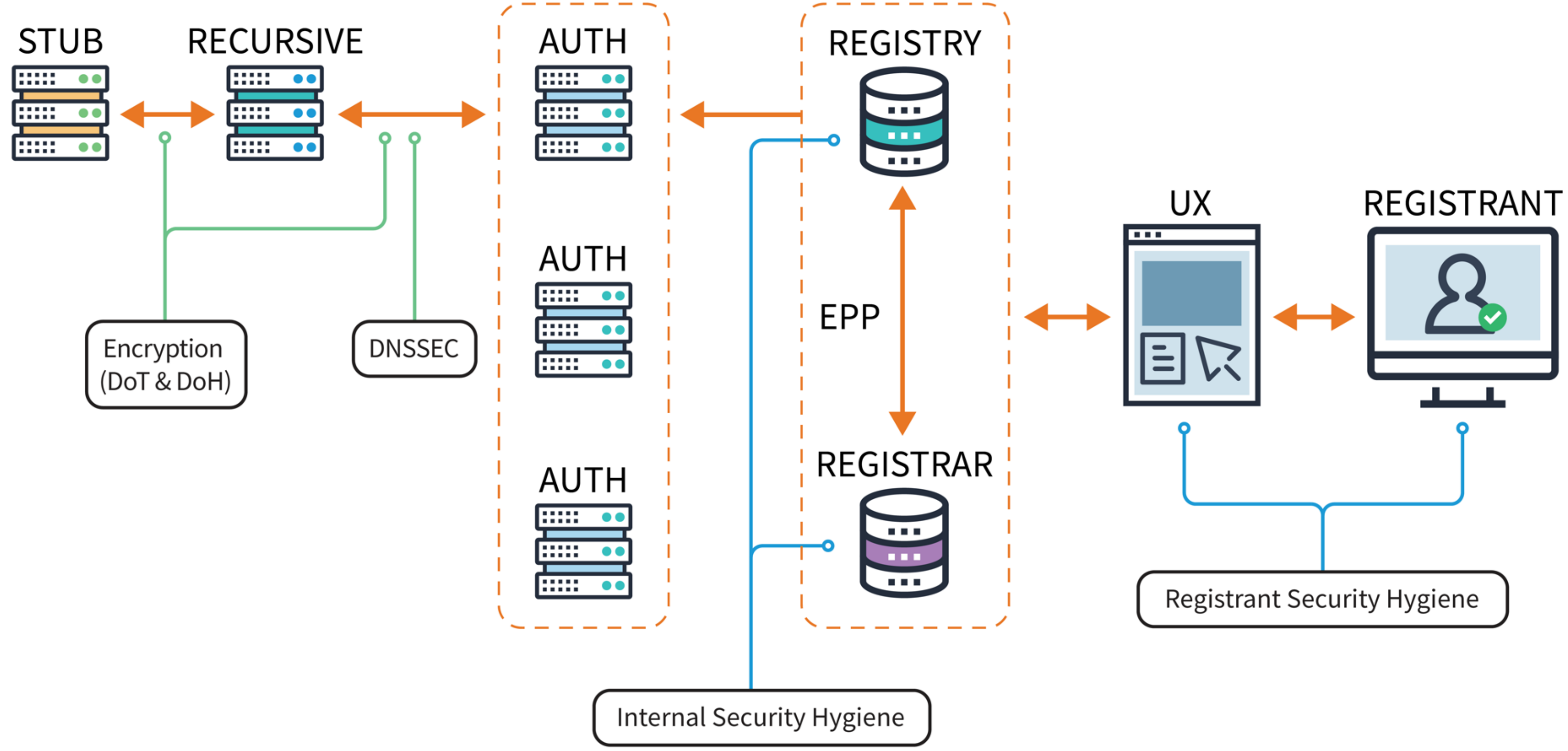
Potential Target Points of the DNS Infrastructure/Ecosystem



TLD registries and domain name registrars provide critical services downstream:

- Registration platform
- Management platform
- Billing platform

A More Secure DNS Ecosystem



Knowledge-sharing and
Instantiating
Norms for
DNS (Domain Name System) and
Naming
Security

….. is pronounced ”kindness.”

KINDNS – Promoting DNS Operational Best Practices

An initiative to produce something simple 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 the industry identifies for better security and more effective DNS operations.

Authoritative DNS Operators of Critical Zones

KINDNS

TLDs & Critical Zones

1. **MUST** be DNSSEC signed and follow key management best practices

2. Transfer 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 authoritative DNS software packages

7. Authoritative servers for a given zone **MUST** run from a diversified infrastructure

8. 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. Transfer 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 a diversified infrastructure

7. The infrastructure that make 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. 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. Recursive servers **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

Public Resolver Operators

KINDNS

This category includes both open and closed public resolvers. Closed public resolvers are typically commercial DNS filtering/scrubbing services, such as DNSFilter and OpenDNS.

Public Resolvers

1. DNSSEC validation **MUST** be enabled

2. QNAME minimization **MUST** be enabled

3. For privacy consideration: Encryption (DoH or DoT) **SHOULD** be enabled

4. Authoritative and recursive nameservers **MUST** run on separate infrastructure

5. Data collected through passive logging of DNS queries **MUST** be limited

6. At least two distinct servers **MUST** be used for providing recursion services

7. Private resolver operators **SHOULD** have software diversity

8. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

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 a multi-factor authentication mechanism

8. Credentials for customer access **MUST** offer two-factor authentication

Self-Assessment & Reports

- Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices
  - Self-Assessments will be anonymous, and a report can be directly downloaded from the web site

- Operators can enroll to participate in one or many categories covered by KINDNS
  - Participation in KINDNS mean voluntarily committing to implement and adhere to agreed norms and practices
  - Participants becomes goodwill ambassadors and promote practices

Self-Assessment Report

KINDNS

Completed on this **09 May 2022**

KINDNS

nstantiating **N**orms for **D**NS and **N**aming **S**ecurity) is
at focuses on the most important operational best
S security best practices.

cursive Resolver Category. The first step in
ce is determining how your server is being

vate?
the open internet (public IP address, not

er the open internet (private IP address, or
tion)

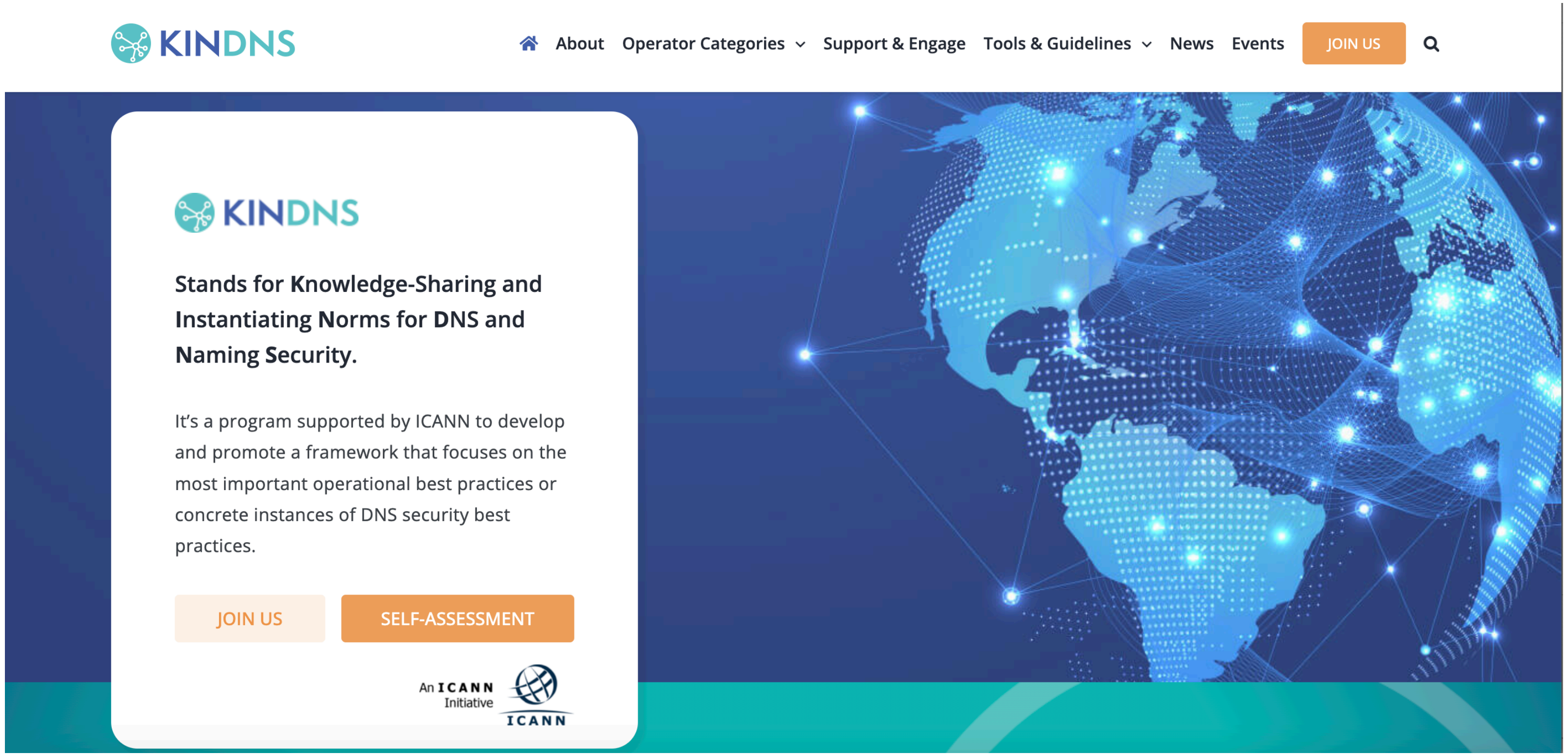
ds to, queries from any client
f some sort to be used (for example, IP
[DoT])

practice, you may be operating one or
and implementation guidelines for
, reflecting the types of resolver

KINDNS

How to Stay Informed and Contribute

- https://www.kindns.org



KINDNS

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.

- **The KINDNS discussion mailing list:** kindns-discuss@icann.org

Engage with ICANN – Thank You and Questions

ICANN

One World, One Internet

Visit us at **icann.org**   Email: champika.wijayatunga@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann