ICANN 73
VIRTUAL COMMUNITY FORUM

# KINDNS

## An ICANN Initiative to Promote DNS Operational Best Practices

**Adiel A. Akplogan**
*VP Technical Engagement*

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

# The Name?

It plays a bit on the Mutually Agreed Norms for Routing Security initiative (MANRS ... pronounced “manners”), so KINDNS is pronounced ”kindness.”

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.

# Key Components of the Current Phase

- Identifying and documenting the most critical security norms for DNS operations (authoritative and recursive resolvers, and software)
  - Consulting and engaging with the operational community
- Developing communications, promotions, and an enrollment plan
  - Developing a dedicated information portal with best practices and implementation guidelines (kindns.org)
  - Enrolling DNS operators to lead by example
- Identifying indicators that will help measure and assess the impact of the initiative
- Mapping best practices to ICANN DNS policy functions (Registry, Registrar, Registrant)

# Categories Covered

- Harden the Operation Environment
  - Services
  - Systems
  - Networks
- **Authoritative Servers**
  - **TLDs and Critical Zone Operators**
  - **SLDs and other**
- **Recursive Resolvers**
  - **Private (closed) Resolvers**
  - **Shared Private Resolvers**
  - **Public Resolvers**
- Privacy Considerations
  - QNAME Minimization
  - DNS-over-TLS (DoT)
  - DNS-over-HTTPS (DoH)
  - ….
- Establish Implementation Guidelines (How-Tos, Checklists, Configuration Processes, Examples)

# Authoritative DNS Operators of Critical Zones

- **Scope/Audience (What are Critical Zones?)**
  - Zones managed by TLD operators/registries, including:
    - TLD zones themselves and subdomains (e.g., co.uk)
    - Any auxiliary zones necessary to the operation of country code top-level domains (ccTLD) (e.g., nic.uk, nic.fr, nic.dk)
  - Other delegation-centric zones of national importance for TLDs
  - SLDs tied to critical services such as healthcare and e-governance/citizen and ID services (e.g., mitid.dk)
  - Finance/banking sites
- **Availability and Resiliency of the DNS Service**
- **Zone File Integrity**
- **DNS Data Integrity and Origin Authentication (DNSSEC)**
- **Architectural Recommendations**
- Network Security
- Host and Service Security
- Customer-Facing Portals and Services (Credential Management)

# Authoritative DNS Operators of Other (SLD) Zones

- **Scope/Audience**
  - All other DNS operators managing DNS services and zones for second-level domains.
- **Availability and Resiliency of the DNS Service**
- **DNS Data Integrity and Origin Authentication (DNSSEC)**
- Network Security
- Host and Service Security
- Customer-Facing Portals and Services

# Recursive DNS Operators

- **Scope/Audience**
  - When considering a recursive DNS resolver, ask the following:
    - Is the resolver service public or private?
    - Is the resolver service open or closed?
  - Clarification:
    - Public DNS resolver services can be reached over the open internet (public IP addresses, not restricted)
    - Private DNS resolver services cannot be reached over the open internet (private IP addresses, or ACL restrictions, or a combination)
    - Open DNS resolvers are reachable by and respond to queries from any client
    - Closed DNS resolvers require authentication of some sort to be used
      - IP address, Transaction signatures (TSIG), TLS certificates (DoT)

- In practice, the following services are found on the internet:
  - **Private Resolvers** – Found in corporate / restricted networks, not publicly accessible
  - **Shared Private Resolvers** – ISPs or similar hosting service providers
  - **Closed and Public Resolvers** – Commercial DNS filtering / scrubbing service
  - **Open and Public Resolvers** – Public DNS resolvers, with no access restrictions

# Recommendations for Private Resolvers

- **Scope/Audience**
  - Private resolvers are normally found on corporate/restricted networks and are not publicly accessible.
  - They are often located on private IP address subnets (RFC1918, for instance), limiting reachability from the rest of the Internet (with or without the use of access control lists/ filters).
  - Private resolvers are in some cases part of a trusted computing domain (Active Directory).
- **Availability and resiliency of resolver services**
- **DNS security – Domain Name System Security Extensions (DNSSEC) Validation**
- Network security
- Host and service security

# Recommendations for Shared Private Resolvers

- **Scope/Audience**
  - Shared private resolver operators are typically Internet service providers (ISPs) or similar hosting service providers.
  - They offer DNS resolution services to their customers (mobile, cable/DSL/fiber residential and commercial users, as well as hosted servers and applications).
  - Access is usually determined by the source IP address of the client or the host that sends the queries. The client or host is using the ISP to access the rest of the Internet.
  - These resolvers are normally shared between many different customers (although an ISP may decide to segment clients based on their type – home/residential DSL and fiber, mobile, commercial).
- **Availability and resiliency of the DNS service**
- **DNS security – DNSSEC Validation**
- Network security
- Host and service security

# Recommendations for Public Resolver Operators

- **Scope/Audience**
  - **Closed and Public Resolvers –** Commercial DNS filtering/scrubbing services (DNSfilter, OpenDNS, etc.).

    These service providers are typically NOT ISPs, and the clients sending the queries are located on remote networks.
  - **Open and Public Resolvers –** "Fully open" public DNS resolvers such as CloudFlare's 1.1.1.1, Google 8.8.8.8, Quad9's 9.9.9.9, etc.

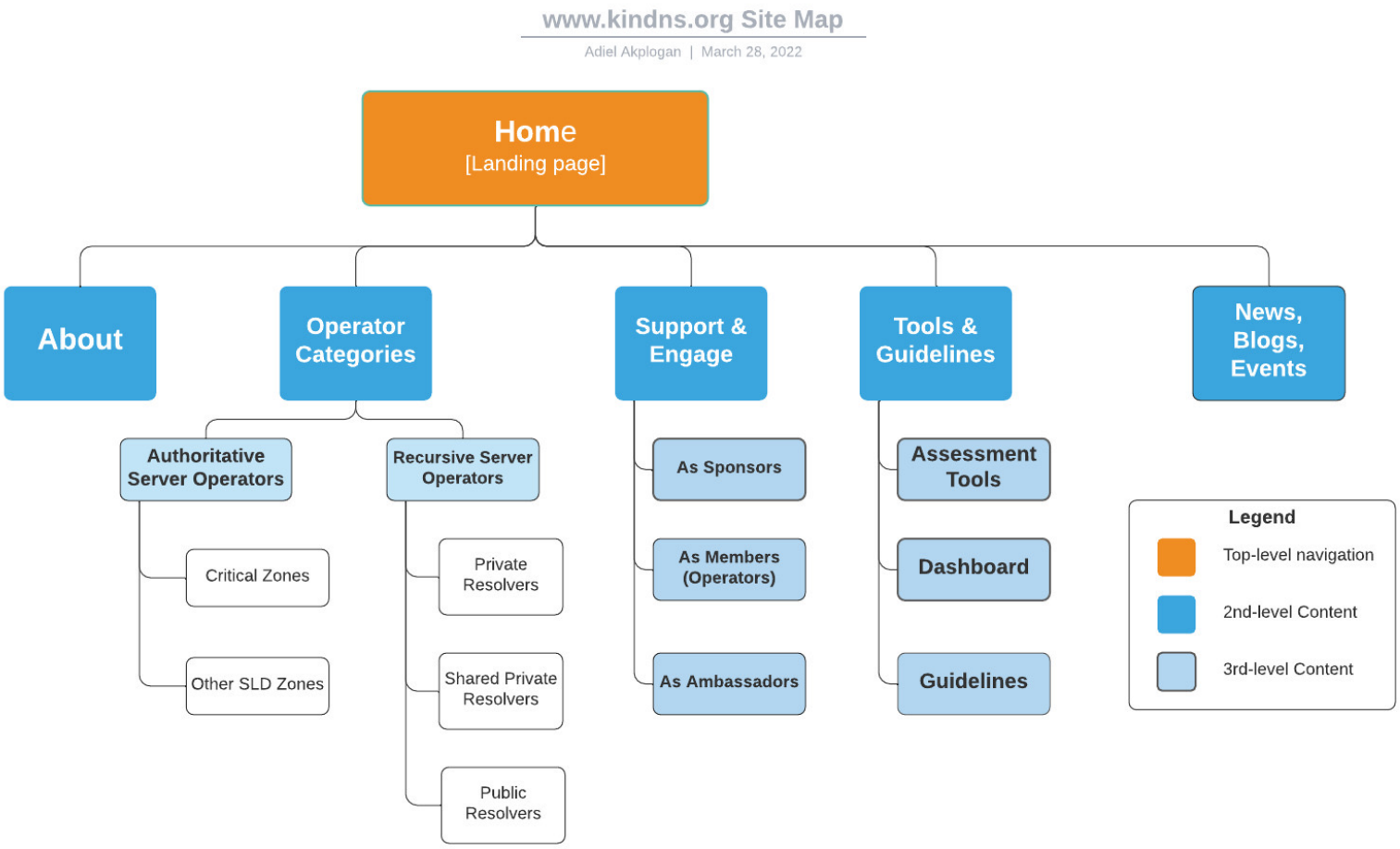
    All users on the Internet are free to use the service, whether they are stub resolvers (clients) or recursive servers using the open resolver as a forwarding service.

- **DNS security – DNSSEC Validation**

- **Privacy consideration**
  - QNAME Minimization
  - DoT
  - DoH

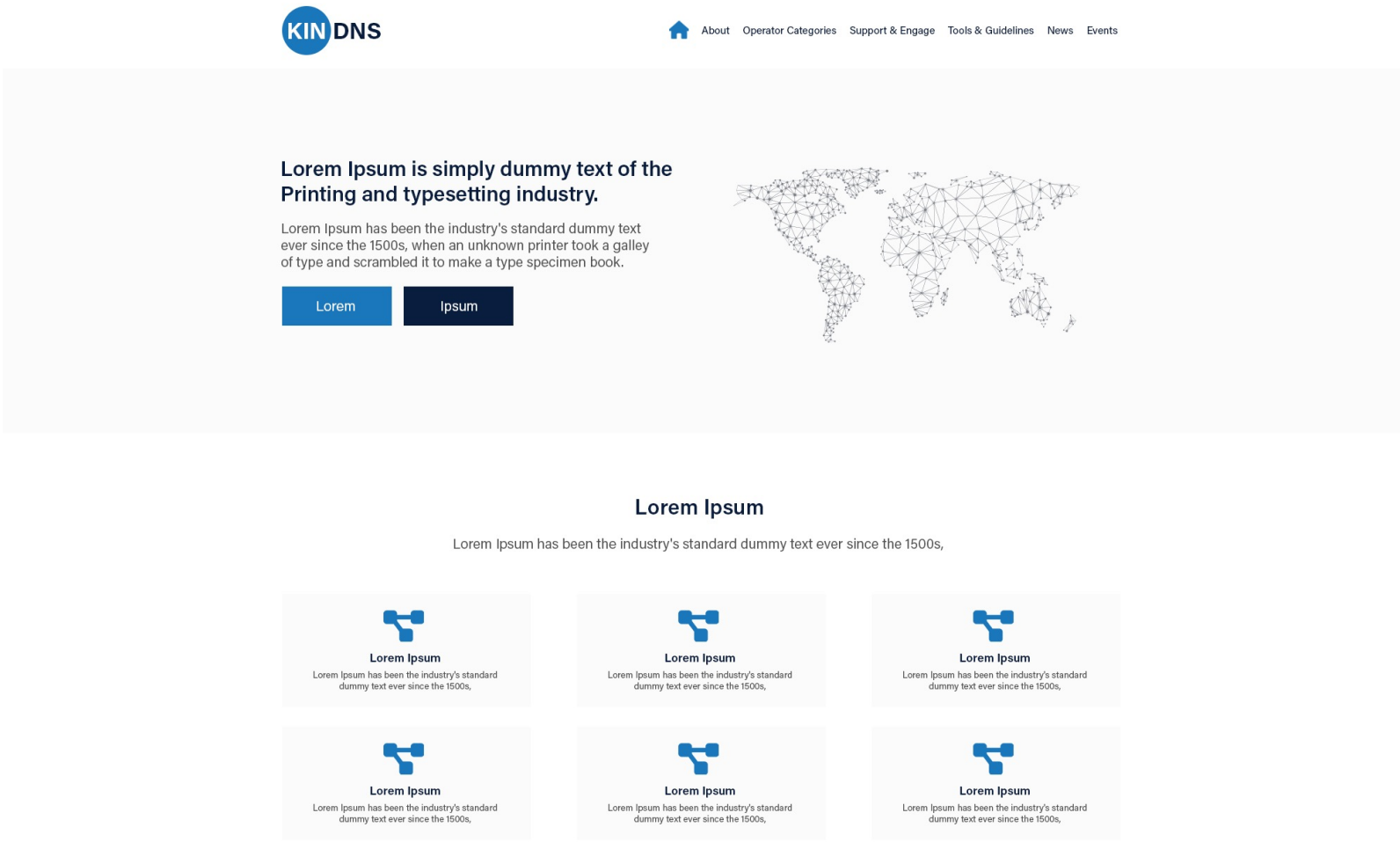
# Web Site Structure

## kindns.org

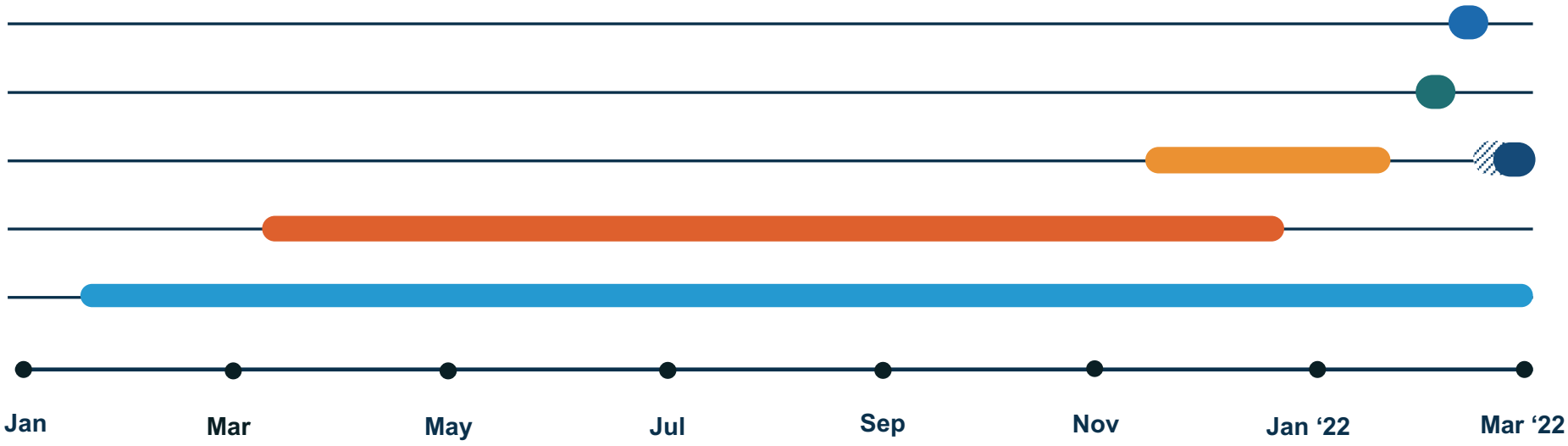


# Web Site Structure

## kindns.org



# KINDNS Timeline




Identify Key Operational Best Practices (BPs)

Develop Implementation Guidelines

Integration of Self-Assessment Tools

Engagement & Community Consultations

Website & Guidelines Published

Soft Launch

Launch

# How to Stay Informed and Contribute

- **The KINDNS discussion mailing list**

  kindns-discuss@icann.org

- We have set up a temporary **Wiki page** where we will share some preliminary documents until the formal website is developed and launched

  https://community.icann.org/display/KINDNS

- **Technical Consultant**: Phil Regnauld

# 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