It Doesn’t Always Have to Be the DNS

A public-health reading of DNS delegation hygiene —
from scanning 8,831 rural U.S. healthcare domains

David Conrad · **SANOG 44 / npNOG 12** · Kathmandu, Nepal · July 2026

the operations haiku

It’s not DNS.
There’s no way it’s DNS.
It was DNS.

Every operator in this room has probably seen/heard/lived all three lines.

// thesis

But was it really DNS?

Many blame the protocol. The evidence blames us.

One interpretation of the haiku

“DNS is fragile — and *of course* it failed.”

We treat the DNS as a flaky black box that betrays us at random.

The hypothesis

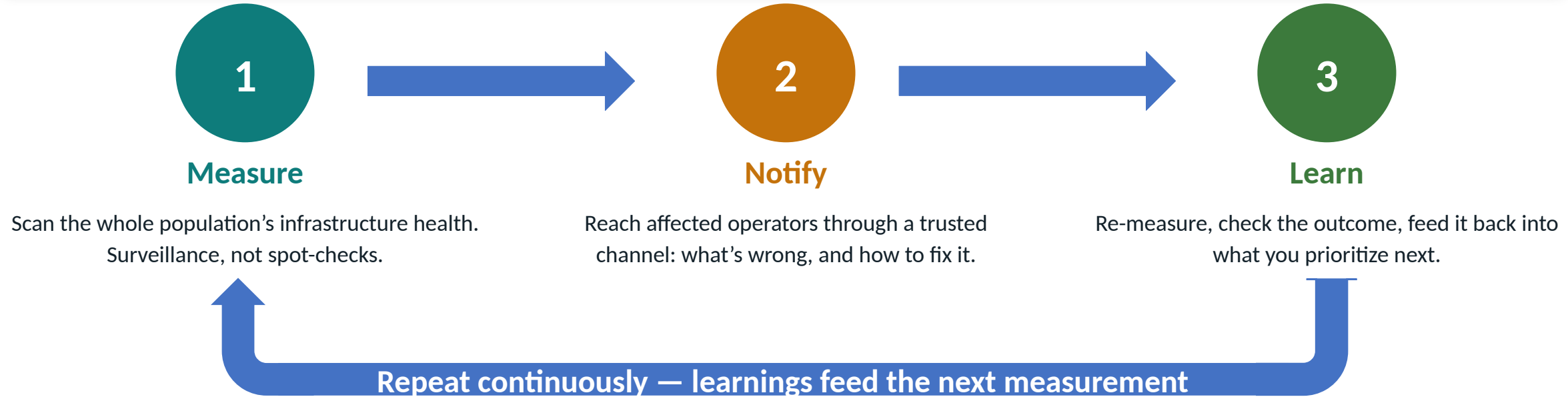
The protocol almost never fails.

What fails is **operational hygiene:** the human-managed infrastructure layers around DNS – who serves the zone, whether parent and child agree, ridiculous and gratuitous complexity, overly permissive software, and whether anyone’s watching.

A different lens: cyber public health

Treat Internet infrastructure risk like population health — shared, systemic, fixed at scale

The core idea: cyber risk **behaves** like a public-health problem: shared, systemic, and **endemic**. You need to treat it across a whole population, not one patient at a time.



Framing: Mulligan & Schneider (2011) and the Cyber Public Health working group.

Where this fits: CyberGreen's Rural Cyber Health Initiative

Pick a population and measure it, find a "trusted notifier" give them the data, and see what works

1 Measure

We chose rural health care, a risky subset of U.S. healthcare facilities, and DNS delegation health as the metric. Scan delegations, score 0 –100, and track over time.

2 Notify

Identify the facilities with the poorest hygiene. Generate a report and send it to Health-ISAC to forward on. Include a survey.

C Learn

Solicit input from Health-ISAC and those that were notified. Goto 1.

PROOF POINT

A notification results in remediation. One Health-ISAC alert took a facility's delegation health from **49.8% → 99.4%** in 4–7 days. Measure, notify, verify — shown operationally real, but this is treating the patient, not the population.

Source: CyberGreen Institute, Rural Healthcare Cyber Resilience Initiative — Phase 2 briefing (2026).

// method

How we measure DNS health at population scale

***Work in Progress**: From "who exists" to a 0–100 delegation-health score for every domain we could find*

A — us-facility-registry
Every U.S. healthcare facility (1.8M+) — the population

B — facurl
Resolve each facility to its real apex domain, if it has one

C — del-checker
Probe each zone, score it 0–100, file findings by severity

What del-checker probes:

- NS-set agreement: parent vs. child
- Reachability over UDP & TCP; EDNS behavior
- Redundancy & diversity: count, ASN, country
- Glue correctness; lame delegations
- SOA sanity; serial consistency across NS
- DNSSEC: DS ↔ DNSKEY chain, algorithms
- Exposure: open resolvers, public AXFR
- And more…

Findings:

CRITICAL	Likely not universally resolvable
HIGH	Significant failure/DoS exposure
MEDIUM	Potential degradation/vulnerability
LOW	Best-practice violation
INFO	Noteworthy; no action required

Scoring:

EXCELLENT	Aggregate Score: 90 - 100
GOOD	Aggregate Score: 80 - 89
FAIR	Aggregate Score: 70 - 79
POOR	Aggregate Score: 60 - 69
CRITICAL	Aggregate Score: 0 - 59

8,831 rural-healthcare domains scanned (so far) · 0–100 health score each · 5 severity tiers

Population-scale, not anecdote-scale — try to think like epidemiologists, not detectives.

// result 1

First, the good news: DNS mostly works (😳)

Ask only “does it resolve?” and the rural healthcare sector looks healthy

94

median health score

86

mean health score

75.8%

rated “Excellent” (≥90)

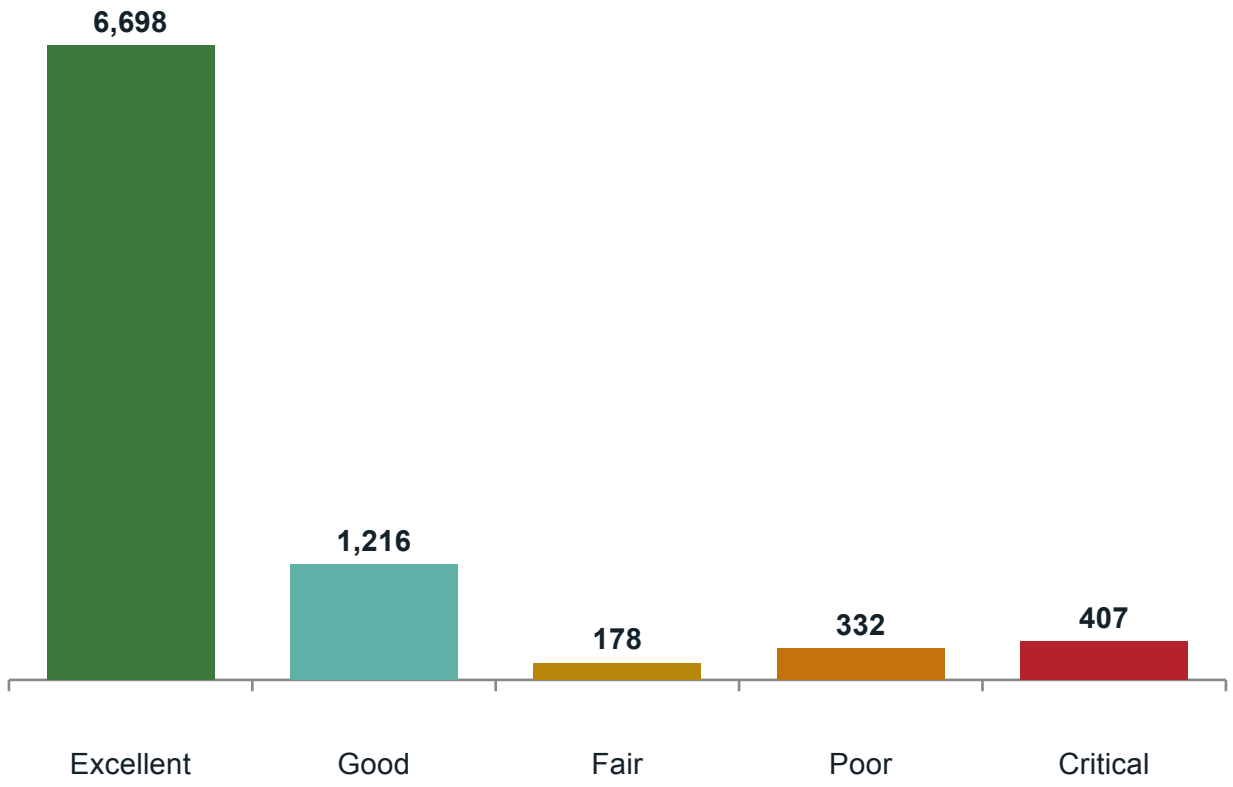
At face value: DNS looks fine.

Three-quarters of these under-resourced facilities score “Excellent.” Queries resolve *(eventually)*, pages load. On an uptime dashboard, nothing here ever turns red.

// result 2

But “mostly works” hides chronic and acute issues

The scores hide a sick tail — and a “healthy” majority carrying chronic conditions



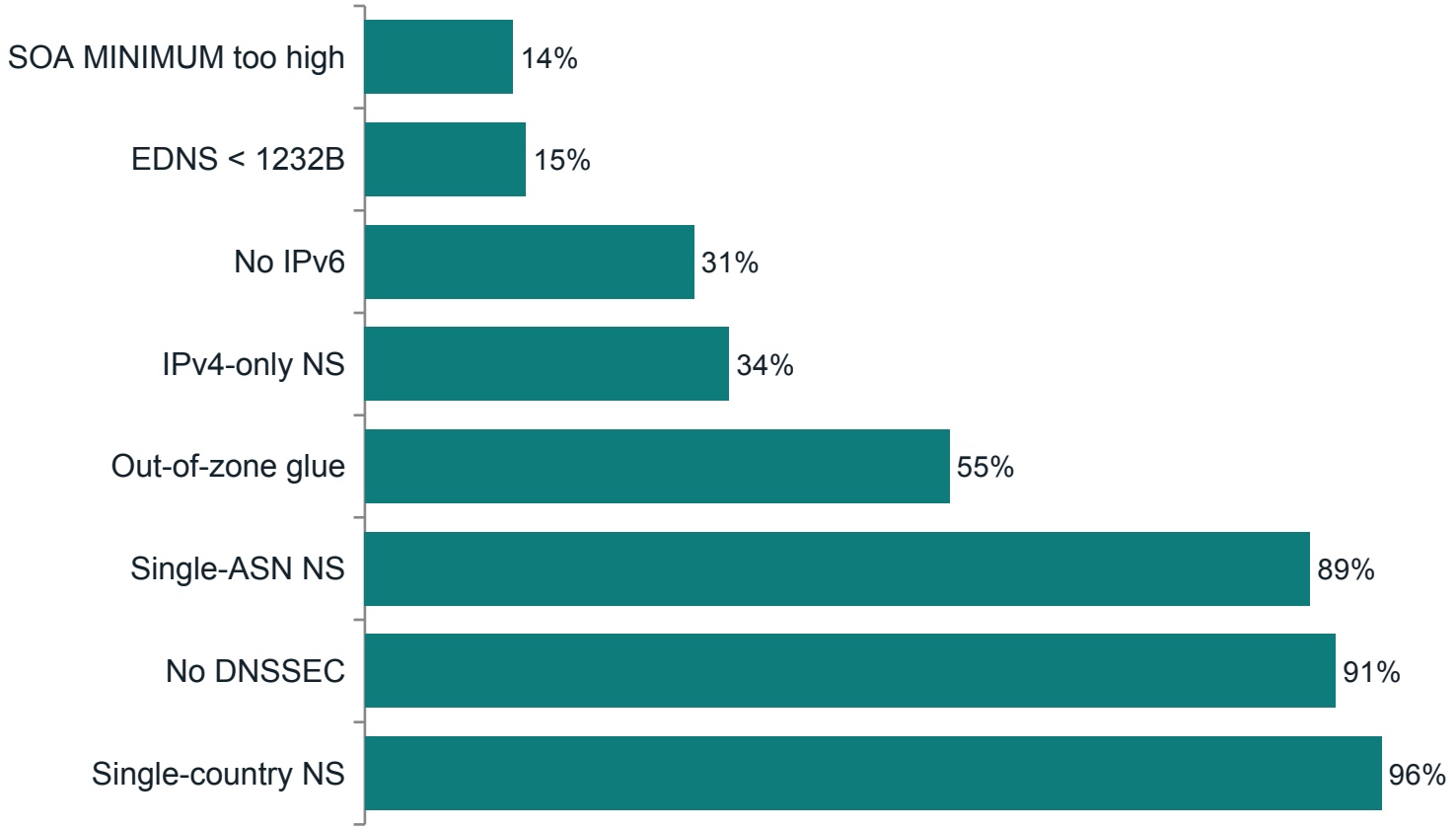
Two problems, not one

The acute tail. 739 domains score “Poor” or “Critical.” 34 flatline at zero.

The chronic majority. Even “Excellent” domains skip DNSSEC and diversity — so common they’ve stopped looking like negative health conditions.

The endemic conditions

Prevalence across all 8,831 domains



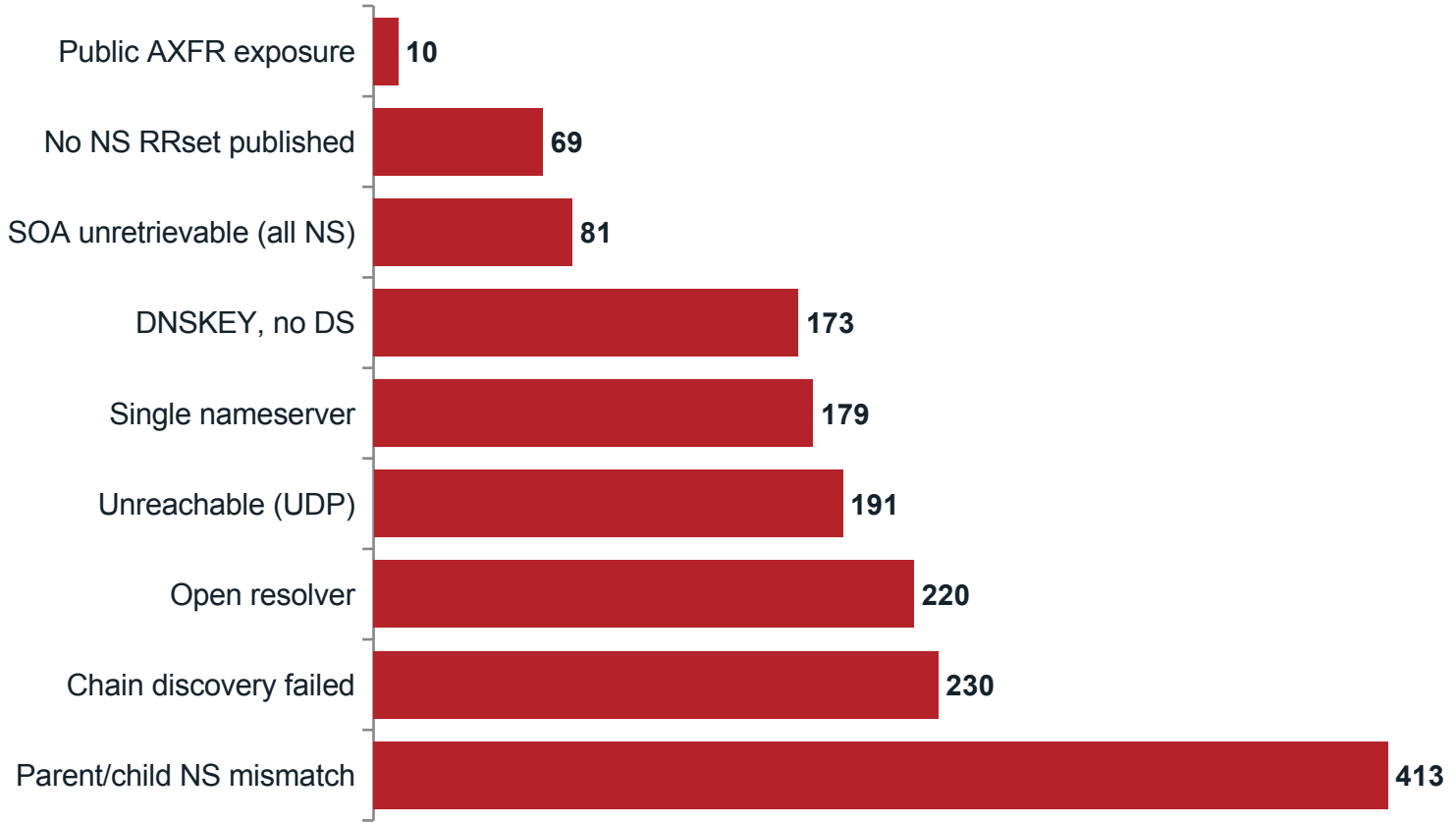
Read it like an epidemiologist

Like blood pressure or cholesterol: (mostly) harmless in isolation but can correlate with bad outcomes.

E.g., none of these pages anyone at 3 a.m. — until one provider, ASN, or region has a bad day.

The acute conditions

Critical & high findings — fewer domains, real danger



593

domains carry ≥1 CRITICAL finding

831

carry ≥1 HIGH finding

It wasn’t DNS.
It was us.

Across 8,831 domains, nearly every serious finding is a human choice — a migration half-done, a default left on, redundancy never bought, a delegation nobody watched. The protocol kept its promises. We didn’t.

So the question isn’t “why is DNS flaky?” It’s “why does a whole sector share the same untreated conditions — and what fixes that at scale?”

02 treating the population

From diagnosis to treatment

We have a lens. Now translate it into action — and weigh the cost of each fix.

Four interventions — and their side effects

Real public-health mechanisms. None is free — I'm proposing, not prescribing.

01

Screening as a public utility

Surveillance

02

Vendor/Provider-level enforcement

Quarantine / gatekeeping

03

Notifiable-disease reporting

Mandatory disclosure

04

Herd immunity via secure defaults

Vaccination

Intervention 1 — Screening as a public utility

Public-health analogy: population surveillance & free clinics

What it means

Run DNS hygiene scanning continuously across a whole sector with notification: a free screening program for DNS. Precedent exists: US CISA's Cyber Hygiene scanning (opt-in) and the UK NCSC's national scanning (opt-out).

The case for it

Reaches operators who'll never hire a DNS expert. Catches endemic conditions early, at near-zero marginal cost.

The case against

You're scanning infrastructure you don't own, maybe unsolicited. Who pays? How do you notify? Who holds the results? On the wire, a friendly scan and attacker recon look identical.

Intervention 2 — Vendor/Provider-level enforcement

Public-health analogy: quarantine & gatekeeping at the border

What it means

Vendors/Providers flag or disallow configurations/delegations that fail basic checks: e.g., parent/child consistency, two reachable servers, no open recursion. Caught at the gate, not years later. Precedent exists: .BANK scans result in a miniscule endemic condition tail.

The case for it

Fixes problems at the one chokepoint every domain must pass through. One registry policy or one provider advisory protects millions downstream.

The case against

Makes vendors/providers judge configs and can result in customer support calls. Overzealous checks after the fact could knock legitimate domains offline: the cure causing the outage.

Intervention 3 — Notifiable-disease reporting

Public-health analogy: reportable conditions for critical sectors

What it means

For **critical** sectors, certain DNS conditions become reportable — hooked into existing frameworks (e.g., US HIPAA-style expectations) so chronic exposure is tracked. Mitigators (e.g., regulators) see prevalence, not just breaches.

The case for it

Make invisible endemic risk obvious. Aggregate reporting reveals the monoculture no single operator can see.

The case against

It may land surveillance and paperwork on the least-resourced. A mandate without funding becomes box-ticking or pushes under-resourced facilities off the internet.

Intervention 4 — Herd immunity via secure defaults

Public-health analogy: vaccination & clean water

What it means

Shift the default: managed DNS/software should ship with automated DNSSEC on, recursion closed, and require two diverse nameservers. Actually implement “Secure by Design”. The under-resourced get a healthy delegation without deciding anything.

The case for it

Highest-leverage fix. Herd immunity works when the safe choice is the automatic one (“Tyranny of the Default”). It reaches the majority who’ll never touch a config.

The case against

Can lead to concentrating everyone onto a few providers, itself monoculture — the single-ASN, single-country fragility we already measure. Curing one disease by spreading another.

// the hard part

The uncomfortable common thread

Every fix collides with the same social determinant: under-resourcing

You can’t “awareness-campaign” your way out of a staffing problem. These facilities didn’t choose bad DNS; it’s a side effect of a larger underlying failure. Any fix that assumes an operator fails exactly where the need is greatest.

Prevention over treatment

Cheaper and kinder than cleaning up outages after the fact. **Scales.**

Defaults over decisions

The only fix that helps people who’ll never make a decision. **Scales.**

Stewardship over blame

In today’s Internet, providers must own population health. Shaming the under-resourced changes nothing.

It doesn’t always have to be the DNS.

The protocol rarely fails. The hygiene around it does — across a whole population, because treating the patient doesn’t scale: you must treat the population.

Measure the population. Prevent before you treat. Make good hygiene the default.

धन्यवाद — thank you. Questions welcome.

Sources & further reading

Framing	Mulligan & Schneider, “Doctrine for Cybersecurity,” Dædalus (2011); Sedenberg & Mulligan, “Public Health as a Model for Cybersecurity Information Sharing,” Berkeley Tech. L.J. (2015).
Cyber public health	CyberGreen / Ostrom Workshop Cyber Public Health WG (Shostack, Ito), cybergreen.net; Google Cloud, “Cyber Public Health” (2024).
Operational precedent	CISA Cyber Hygiene Services (free scanning); UK NCSC “Scanning Made Easy” / Active Cyber Defence.
DNS standards	RFC 1034/1035 (delegation); RFC 1912 (common errors, lame delegation); RFC 2182 (diverse secondaries); DNS Flag Day 2020 (EDNS 1232B).
Exposure	CISA TA13-088A (DNS amplification / open resolvers); CISA TA15-103A (AXFR zone-transfer leakage).
Sector context	HIPAA Journal 2024 healthcare breach review; HHS OCR breach portal; AHA 2024 cybersecurity outlook.
Data	del-checker delegation scan of 8,831 U.S. rural healthcare domains, run 2026-07-08 (this talk).