Aldrich SOLUTIONS®

Your Network Your Risk

A FIELD-READY CYBERSECURITY PLAYBOOK FOR RURAL BROADBAND OPERATORS

JOSH AXELROD | WTA FALL EDUCATIONAL FORUM | OCTOBER 6, 2026

Copyright © 2026 Aldrich Services LLP. All rights reserved.

About This Session

- This presentation is for education only. It is not legal, regulatory, audit, or investment advice, and it does not create a client relationship.
- The presenter is affiliated with Aldrich, a professional services firm that provides audit, tax, and advisory services. Nothing in this session is an offer of, or a recommendation to obtain, those services.
- No products or vendors are endorsed. Statistics come from the public sources named on each slide.
- The live demonstration uses a fictional organization and simulated data. No real systems were scanned.

- **Consult your own counsel and advisors about your specific obligations.**

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

6:47 PM on a Friday

- A 40-employee fiber cooperative gets an automated alert: their billing portal is running slow. IT assumes a vendor-side issue and goes home.
- By 9:15 PM, an employee's credentials — harvested three months earlier through an infostealer infection nobody detected — are used to log into the VPN. By midnight, the attacker has mapped the network. By 4:00 AM, ransomware locks the billing system, the customer database, and two field-service laptops.
- The company doesn't pay. They rebuild from backups. It takes 11 days to fully restore billing — during which they can't process payments, can't confirm outages accurately, and miss a USAC compliance filing deadline.
- **No system was "hacked" in the movie sense. A credential leaked, and nobody saw it or couldn't. That's the type of gap this session works to close.**

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Today's Agenda

- Why Telecom, Why Now
- Your Funding, Your Risk
- The Framework: Map → Prioritize → Harden → Sustain
- Live Demo: AI-Assisted Defensive Recon
- Your Action Plan, by Tier

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Telecom Is the Target

May 2023

Volt Typhoon disclosed

China-linked actors hiding in U.S. critical infrastructure, including communications.

Feb 2024

CISA, NSA, and FBI advisory AA24-038A

Volt Typhoon held access for at least five years.

Late 2024

Salt Typhoon breaches

Breaches of at least eight U.S. carriers become public; call records exposed.

Jan 16, 2025

FCC rule

FCC rules that CALEA requires carriers to secure their networks.

Aug 27, 2025

13-nation advisory AA25-239A

Entry through known, unpatched routers, firewalls, and VPNs.

Nov 20, 2025

FCC rescinds

FCC rescinds the ruling 2–1, relying on voluntary carrier commitments.

The way in was known, unpatched edge gear.

Sources: CISA AA24-038A (Feb 2024); CISA/NSA/FBI AA25-239A (Aug 2025); FCC orders (Jan 16 and Nov 20, 2025). Dutch MIVD/AIVD reported smaller ISPs' routers were also accessed (Aug 2025).

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Security Operations Aren't Keeping Pace

- Patching: median time-to-patch rose from 32 to 43 days, just as vulnerability exploitation became the #1 way attackers get in (31% of breaches)
- Vendor and access reviews rarely happen when a new AI tool or data center partner is added
- Credential monitoring is seldom in place, though 73% of ransomware victims had a credential leak the year before
- Incident response plans, where they exist, are often untested
- **Practices are sized for yesterday's network, not the one you're building today**

Source: Verizon 2026 DBIR

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Phase 1 Builds. Phase 2 Monetizes.

- **Phase 1 — Build**
- BEAD-funded fiber buildout
- 2026 bonus depreciation pulling capex forward
- New entrants and doubled footprints
- **Exposure: new segments, field gear, vendors**

- **Phase 2 — Monetize**
- Regional colocation and edge data centers
- Co-op power and land as data center assets
- AI-enabled planning and operations
- **Exposure: tenants, partners, AI tools with system access**

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Growth Is Outpacing Security Maturity

- Every new revenue line — colocation tenants, AI planning tools, data center partnerships — is a new vendor and a new integration point
- Third-party breaches jumped 60% in one year and now account for 48% of all breaches
- Most rural operators are adding these relationships without dedicated security staff to vet them
- **Each one belongs on your threat surface map before it goes live**

Source: Verizon 2026 DBIR

Copyright © 2026 Aldrich Services LLP. All rights reserved.

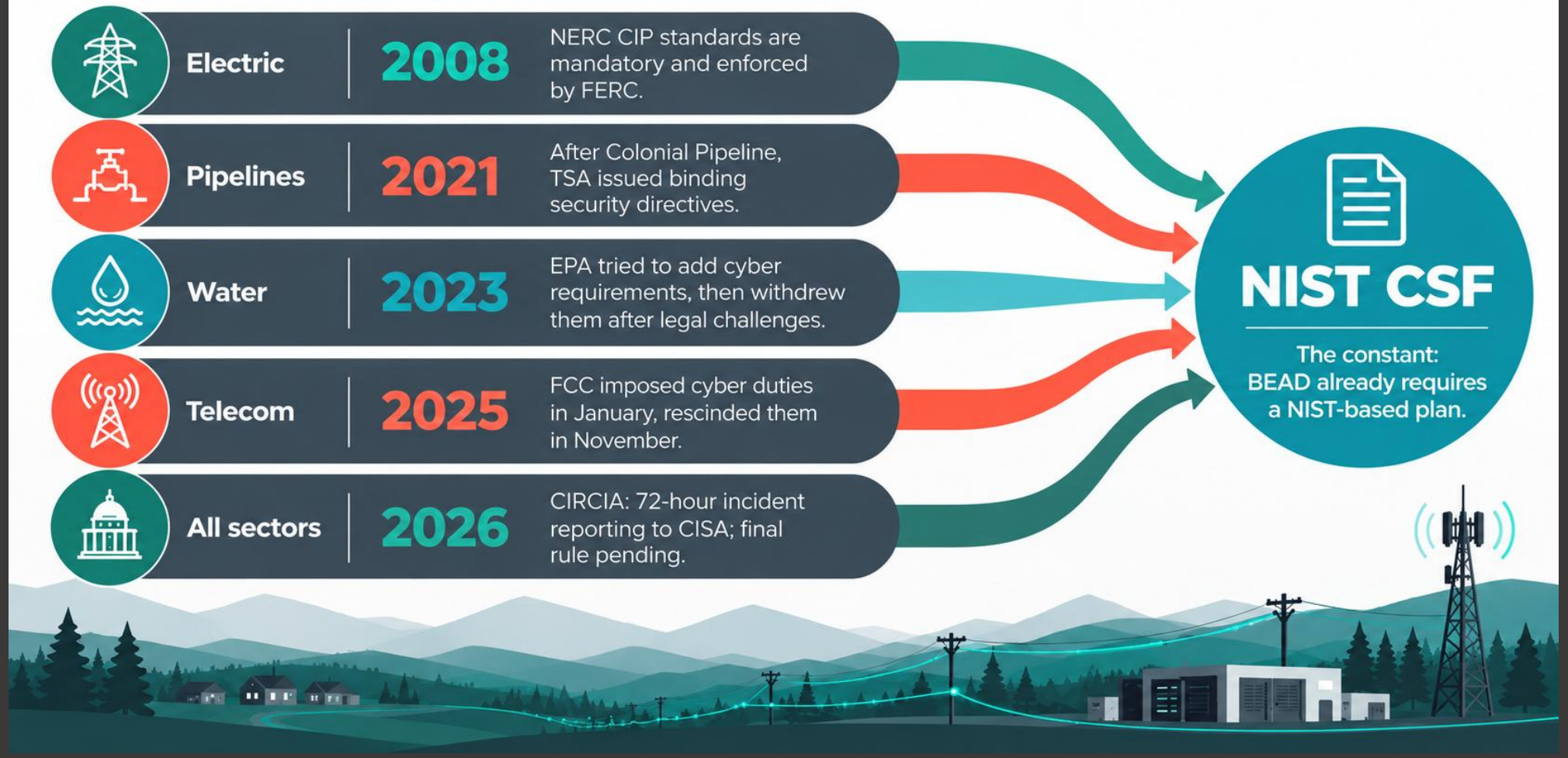
Your Funding, Your Risk

- BEAD subgrantees must attest, before funds flow, to an operational cybersecurity plan reflecting the latest NIST Cybersecurity Framework
- They must also attest to a supply chain risk plan based on NIST IR 8276 and SP 800-161
- The requirement survived the June 2025 BEAD restructuring and remains in NTIA's November 2025 grant terms
- If you buy wholesale carriage, your network provider must attest too
- **An attestation you can't back up is its own risk. Review yours with counsel.**

Source: NTIA BEAD General Terms and Conditions (Nov 18, 2025)

Copyright © 2026 Aldrich Services LLP. All rights reserved.

How Regulation Reached Other Sectors.



Sources: FERC Order 706 (2008); TSA Security Directive Pipeline-2021-01; EPA (Oct 2023); FCC (Jan 16 and Nov 20, 2025); CISA CIRCIA rulemaking; NTIA BEAD terms (Nov 18, 2025).

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

A Practical Framework for Rural Operators

A repeatable cycle to reduce risk, meet requirements, and enable growth.

1 Map

- Inventory assets, data, vendors
- Map connections and dependencies
- Identify critical services
- Define your current risk posture

2 Prioritize

- Assess threats and vulnerabilities
- Focus on highest-impact risks
- Consider regulatory and business priorities
- Build a realistic roadmap

3 Harden

- Implement prioritized controls
- Patch, configure, and segment
- Strengthen identity and access
- Secure vendors and supply chain

4 Sustain

- Monitor and detect
- Test plans and train your team
- Review vendors and access
- Measure progress and improve

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Five Categories Every Rural Operator Should Map

Network Edge & Field Gear

Billing & OSS/BSS Systems

Customer Data & CPNI

Compliance Systems (USAC/E-Rate)

Third-Party & AI Tool Access

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

The Threat Surface Mapping Worksheet

Asset Category	System	Data Handled	Current Controls	Owner	Last Reviewed
Billing & OSS/BSS	Billing Portal	Payment & account data	Password only, no MFA	IT Lead	Not yet reviewed

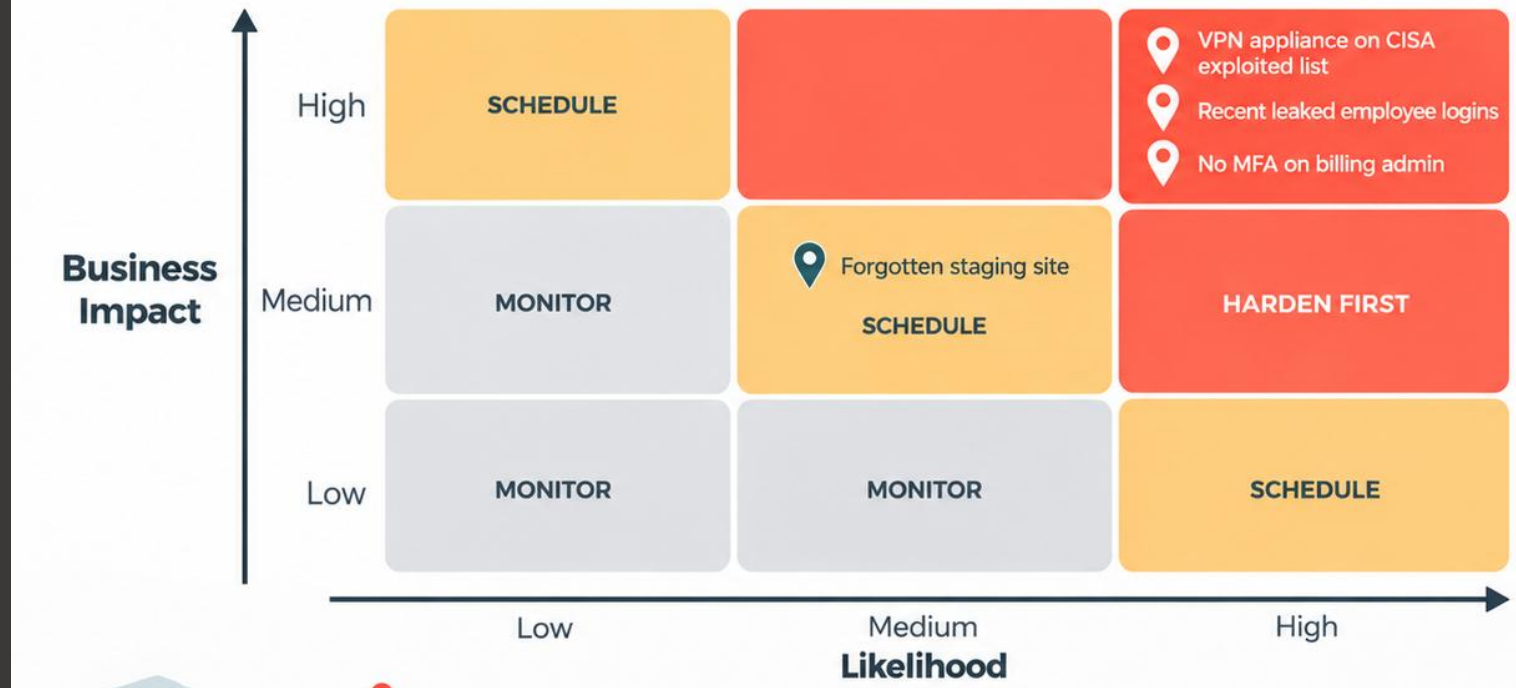
This worked example flags a top-priority gap: no MFA on a billing-critical system.

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Score Risk Like a Business Decision.

Likelihood × business impact, not technical severity alone.



What Impact Means for a Rural Telco

Low
Contained, no customer-facing effect

Medium
Localized outage, recoverable within a day

High
Billing or network-wide outage, customer data exposure, or a compliance failure

Anything in the top-right corner is where Harden starts.

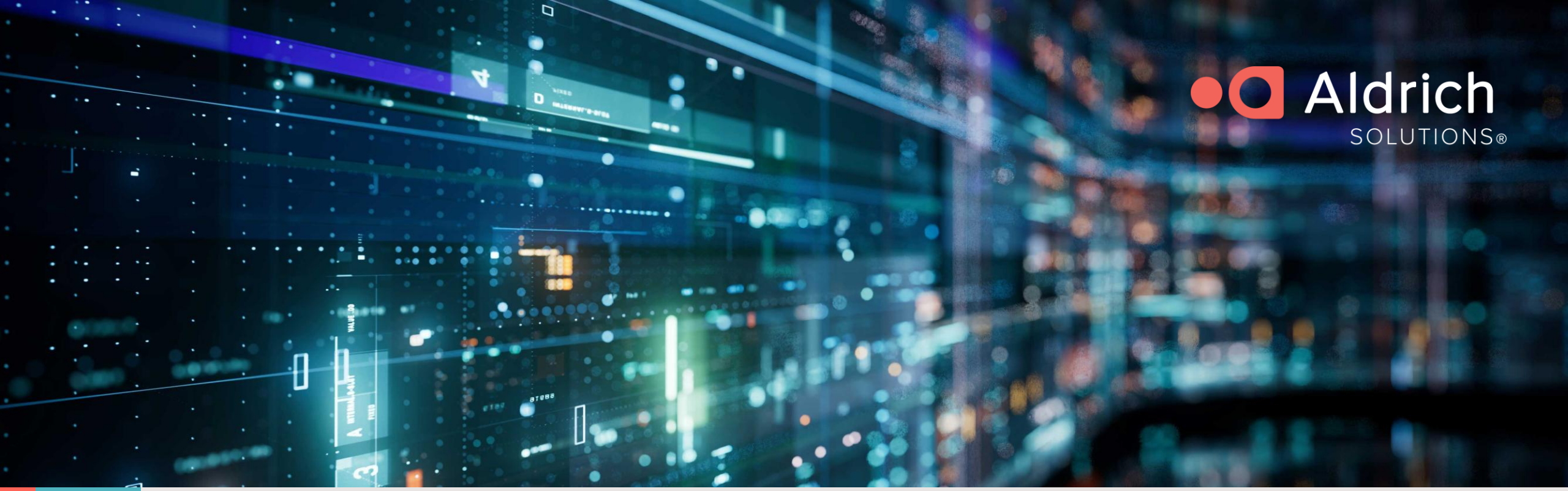
Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Harden, Then Sustain

- Patch internet-facing routers, firewalls, and VPNs first, starting with CISA's Known Exploited Vulnerabilities list
- Require MFA on all remote and admin access, including vendor and MSP accounts
- Review vendor access whenever a new partner, tenant, or AI tool connects
- Write and test a one-page incident plan for the first 72 hours
- **Re-run the cycle quarterly and keep your cyber and supply chain plans current**

Copyright © 2026 Aldrich Services LLP. All rights reserved.



Aldrich SOLUTIONS®

Live Demo: AI-Assisted Recon

FICTIONAL CO-OP | SIMULATED DATA | NOTHING IS SCANNED

Copyright © 2026 Aldrich Services LLP. All rights reserved.

SEEING YOUR NETWORK THE WAY AN ATTACKER DOES

What you'll see

An AI assistant reviewing a fictional rural co-op's public footprint, using the same passive sources an attacker would.

Authorized and simulated

The target is fictional and nothing is scanned. Run this only on assets you own or are authorized in writing to assess.

Copyright © 2026 Aldrich Services LLP. All rights reserved.

The AI-Assisted Recon Workflow

- Authorize and scope: your domains, IP ranges, and brand names, in writing
- Discover passively: certificate logs, public DNS, search indexes, breach alerts
- Let AI synthesize: cluster findings and rank the most likely way in
- Flip to defense: score each finding by business impact
- Fix and repeat: quarterly, and after every new vendor or AI tool

Copyright © 2026 Aldrich Services LLP. All rights reserved.

What to Check Monday Morning

- List every internet-facing router, firewall, and VPN, and confirm its patch level
- Check that list against CISA's Known Exploited Vulnerabilities catalog
- Turn on breach alerts for your company email domain
- Search for public documents that reveal your network, vendors, or org chart
- Review which staff details are public and useful for a phishing pretext

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Telecom add-ons for every tier: patch edge devices against CISA's KEV list, keep BEAD cyber and supply chain plans current, and see the companion playbook for tier detail.

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Your Leave-Behind: The Companion Playbook

Tool 1
Threat Surface Mapping Worksheet

Inventory systems, data, controls, and owners across five telecom categories. Edge devices first.

Tool 2
Risk Prioritization Matrix

Score each gap by likelihood and business impact using rural-telco impact definitions.

Tool 3
Action Plan by Tier

The 30/60/90 plan for your tier, with owner and status columns plus telecom add-ons.

Tool 4
AI-Assisted Recon Checklist

The five-step demo workflow your team can run quarterly on assets you own.

Also inside: how to pick your tier, how the tools support your BEAD cyber and supply chain attestations, and a dated resource appendix.

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Aldrich SOLUTIONS®

Where to Go Next, at No Cost

- NTCA CyberShare: the Small Broadband Provider ISAC
- CISA advisory AA25-239A (Salt Typhoon) and the Known Exploited Vulnerabilities catalog
- NIST CSF 2.0 (Feb 2024) and its Small Business Quick-Start Guide
- NTIA BEAD cybersecurity and supply chain guidance, plus your state broadband office's plan templates
- Verizon 2026 Data Breach Investigations Report

Copyright © 2026 Aldrich Services LLP. All rights reserved.

If You Remember One Slide, Remember This One

- Telecom is a named target, and the way in is edge gear you already run
- If you took BEAD money, you attested to a NIST-based plan. Make it real.
- Regulation will swing. NIST is the constant worth building on.
- Score risk by business impact, then run the cycle every quarter
- Start at your tier. You need an owner and a process, not a security team.

Copyright © 2026 Aldrich Services LLP. All rights reserved.

Thank you.

Questions and discussion