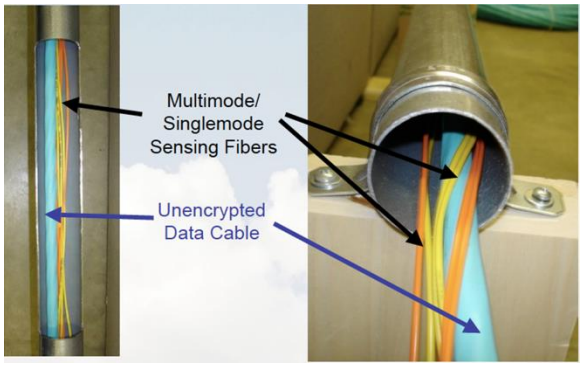
1. Security Philosophy: ZeroTRUST Privacy Assured Link "PAL" vs. "PDS" Protective Distribution System U.S. Gov CNSSI 7003

Apriori Network System – "Privacy Assured Link"

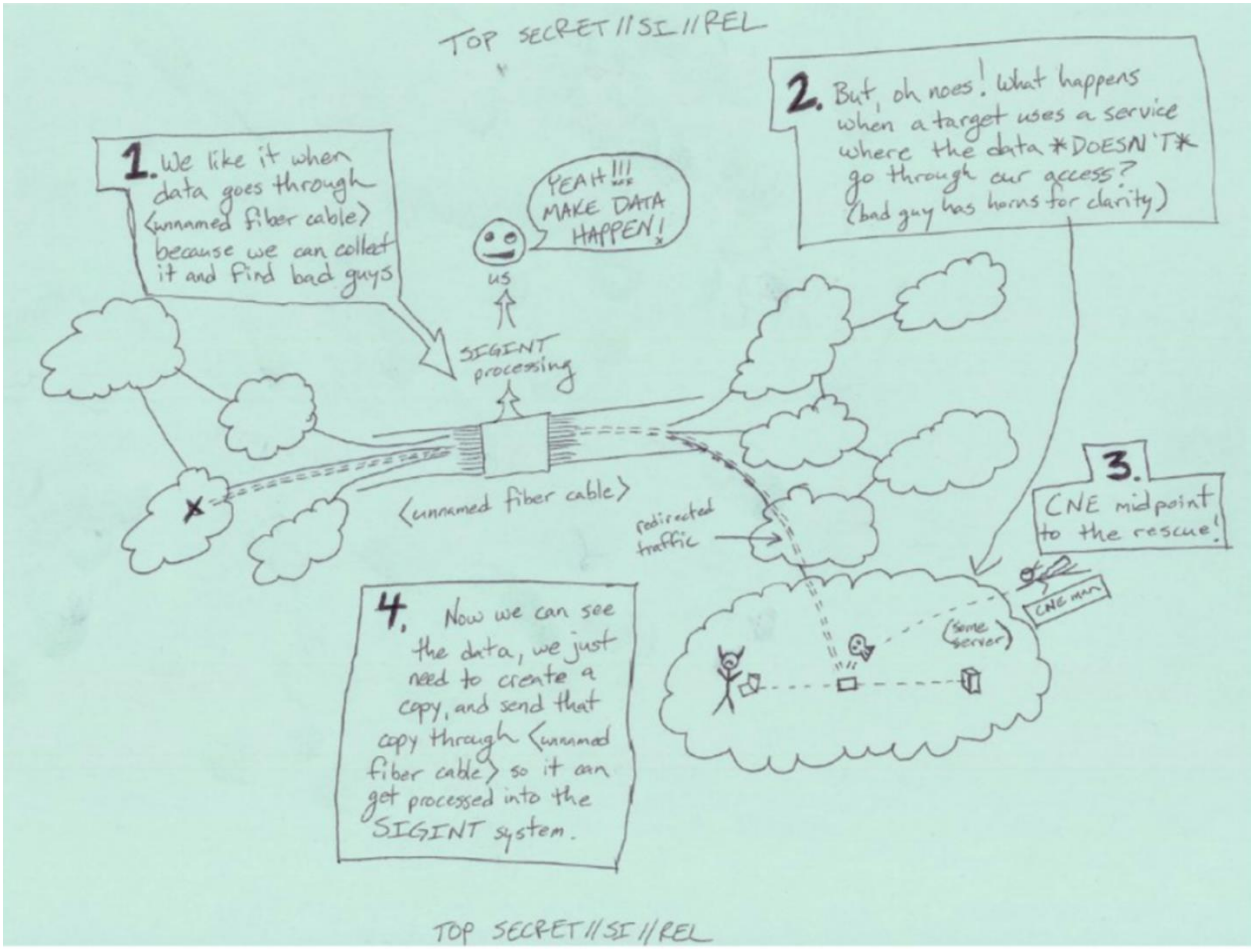
- Design Philosophy: Built from the ground up for privacy-by-design with inherent security at the physical layer.
- Core Feature: Utilizes single-strand, single-mode, 5 or 7 Multi-Core ("MCF") optical fiber with intrinsic, defensive "chaff" generation, patented torrents of optically modulated data transmitted into surrounding cores disabling the hacker's capabilities to acquire the targeted transmission data being received and/or sent. The patented, pluggable endpoints also have embedded detection sensing of signal disturbance or eavesdropping (via changes in light characteristics or quantum-safe protocols).
- Best Use Case: Perfect for high-assurance single-user or low-count links, such as remote office connections in shared buildings, where tenants need assurance that no cross-tenant data snooping is possible.
- Advantage:
    - Minimal infrastructure footprint –a dangerously smart patch cord: set & forget and sleep at night knowing data traversing that path is safe.
    - Ideal for existing multi-tenant environments where you can't enforce PDS on others.
    - Not conspicuous, looks and feels like single strand fiber.
    - Tamper-evident transmission path by design
    - Stealthy and cost-effective

CNSSI 7003 PDS (Protective Distribution System)

- Design Philosophy: Focuses on physical protection of cables against unauthorized access/tapping.
- Core Requirement: Cables must be installed in secure, monitored conduits or hardened pathways.
- Best Use Case: Well-suited for enterprise or DoD campuses with centralized fiber runs carrying large bundles—e.g., 48, 72, or 144 fiber-count trunk lines.
- Advantage:
    - Standardized and vetted for classified data
    - Ideal when you control the building or pathway infrastructure
    - Scales well with high fiber-count backbones



2. The Real Problem:



This is where Apriori's approach shines: **Offices in Multi-Tenant Buildings**

Challenges:

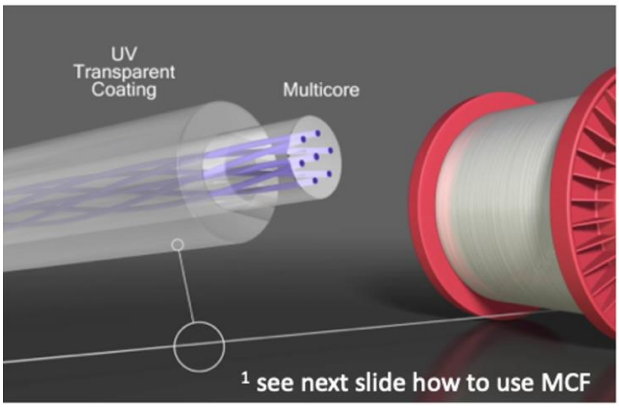
- Tenants don't control the building wiring closets, cable trays, or who shares the riser.
- Other tenants could be competitors, hostile actors, or simply careless.
- CNSSI 7003 can't be enforced without full control of the premises.
- Tapping fiber without detection is **a real risk** in these settings.

Apriori's Advantage:

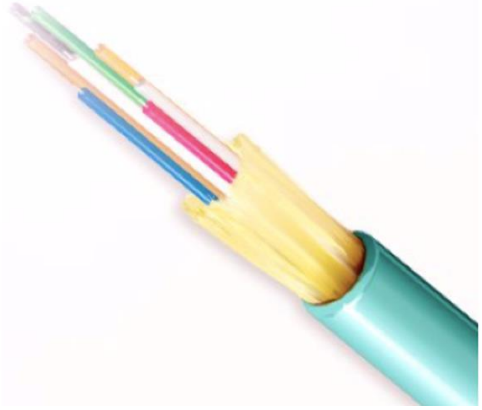
- Using **single-strand fiber** that can detect tampering means:
  - You don't rely on conduit security—you rely on **transmission integrity**.
  - Zero added latency: no encryption, no interaction within data.
  - Data security is intrinsic, all within the fiber's outer cladding outer cores.
  - **No need to trust** shared pathways.
  - You can **prove your link is secure or alert when it's not**.

3. Fiber Count Optimization

Multi Core Optical Fiber[1] (MCF)



Industry's Current Term Multicore Fiber



Use Case	Best Option	Reasoning
Single user in shared office	Apriori	Least infrastructure, built-in privacy, no trust needed in environment
Campus-wide secure backbone	CNSSI 7003	Economical for many fibers, centralized security monitoring
Multi-tenant, remote branches	Apriori	Secure even if you're one tenant among dozens—non-intrusive deployment
Government SCIF facilities	CNSSI 7003	Mandated PDS standard, manageable with total physical control

Summary: Why Apriori Excels for the Current Landscape

In today's reality:

- Remote work is standard.
- Multi-tenant buildings are common.
- Control over infrastructure is limited.
- Trust is not assumed.

That makes Apriori's Privacy Assured single-fiber solution the most practical **and scalable answer** for securely connecting remote offices without needing physical control of the entire building.

Meanwhile, CNSSI 7003 Protective Distribution System remains the gold standard for centralized, high-security environments with full physical control.