OT-ISAC
OPERATIONAL TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS ISAC

Thought Leadership in Threat Intelligence Sharing

IA

Ian Andriechack

CEO, **ALLITSystems LLC** | **OTICS-ISAC**

Published November 2025

The IT Interview Question That Explains Why We Need More ISACs, Not Fewer

I remember my first real IT job interview like it was yesterday. Sitting across from the hiring panel in a paramilitary corrections environment, palms sweating, I was asked a deceptively simple question: "Andriechack, what's your take on IT?"

The question was so broad it could have stopped me in my tracks. Instead, I found clarity in a truth that has defined my entire career: **"No one knows everything about IT. It's just not possible with how fast the industry grows. The difference between a real IT-oriented individual and others is that IT people are constantly trying to stay ahead, grow, and learn as much**

as they can."

My answer wasn't polished. I stumbled through it, and the sweat on my palms didn't lie about my nerves. But the core message resonated because it was honest. IT is vast, complex, and ever-changing. Specialization isn't a weakness; it's our greatest strength.

Today, as I work with multiple ISACs, ISAOs, and threat intelligence organizations, I see an exciting opportunity that the cybersecurity community is missing. We're being told that generalization is the answer, that existing ISACs can serve all sectors if we just leverage them properly. As the IT-ISAC argues, "instead of investing time and resources to create a new organization to do what is already being done, it might be more effective for the government to better leverage existing structures to share threat intelligence."[1]

But I believe we can do better. Much better.

The Fundamental Opportunity

In August 2025, the IT-ISAC published an article arguing against the creation of a proposed AI-ISAC. Their central argument was that AI threats are simply another tool in an attacker's arsenal, and that creating specific ISACs for each attack vector would be inefficient when existing ISACs already monitor and share intelligence about AI-enabled threats.[1]

> **But here's what I believe this perspective misses: The call for specialized ISACs has never been about threat vectors like AI-enabled attacks or OT/ICS compromises. It's about sectoral context.**

There are two entirely different dimensions of cybersecurity:

Dimension 1: HOW you're attacked. Tools and techniques (ransomware, AI-orchestrated campaigns, OT/ICS exploits)

Dimension 2: WHY, WHERE, and WHAT makes you a target. Your sector's unique regulations, operational constraints, adversary landscape, and stakeholder obligations

In my experience, single ISACs serving multiple disparate sectors simply cannot develop deep expertise across all of them. Cannabis operations have nothing in common with hospitality operations, which share no operational context with legal services or municipal recreation systems. Each sector has fundamentally different threat landscapes, regulatory frameworks, and operational

constraints.

The Uncomfortable Truth About Umbrella ISACs

Let me be direct about what I see happening when existing ISACs argue against creating sector-specific organizations: **This raises questions about whether the focus is on market expansion rather than mission effectiveness.**

When established ISACs suggest that corrections facilities, cannabis businesses, legal services firms, municipal recreation systems, and food and agriculture operations should all join their existing membership rather than forming specialized ISACs, it looks like a business development pitch. Every new sector-specific ISAC represents organizations that won't be paying membership dues to the umbrella organization. This is particularly concerning for agriculture and other sectors that rely heavily on OT/ICS systems, where the operational context is critical to understanding threats.

The question I keep asking is: Are ISACs service organizations dedicated to protecting their sectors, or are they membership-based businesses optimizing for revenue growth?

Consider what I believe umbrella ISAC expansion really means:

Corrections facilities paying membership fees for generic intelligence that doesn't address contraband phone detection vulnerabilities, door control system compromises, or constitutional compliance requirements unique to corrections.

Cannabis businesses paying for intelligence that ignores cash-based operation security, HVAC control systems for grow operations, federal-state legal conflicts, and seed-to-sale tracking system vulnerabilities.

Legal services firms paying for intelligence that doesn't understand attorney-client privilege constraints, opposing counsel threat actors, or court deadline pressures.

Municipal recreation systems paying for intelligence developed for enterprise IT budgets that don't translate to public sector pool filtration controls, HVAC systems, or facility access constraints.

Food and agriculture operations paying for intelligence that doesn't account for precision agriculture IoT vulnerabilities, autonomous equipment security, supply chain integrity, weather-dependent operational constraints, or the unique intersection of OT/ICS systems with food safety requirements.

In my view, these sectors would be paying for inadequate service rather than building the specialized intelligence sharing they actually need.

The firms supporting these underserved sectors (corrections vendors, municipal IT contractors, cannabis technology providers, legal practice management companies, agricultural technology providers) are typically small operations, many already resource-constrained. They don't have capacity for dedicated security teams with deep expertise. They rely on a handful of experienced professionals who understand both the technology AND the sector context. The talent pool of people who understand both cybersecurity AND corrections operations, cannabis compliance, legal ethics, or precision agriculture is small and specialized.

When we force these sectors into umbrella ISACs driven by membership growth rather than sectoral expertise, I believe we're choosing profit over community protection.

The Same Attack, Completely Different Contexts

Here's what excites me about sectoral specialization: When we understand context, we can provide truly actionable intelligence. Consider **ransomware** across different sectors:

IT Company

- **Response:** Failover to redundant systems, restore from backups
- **Timeline:** Hours to days
- **Concern:** Business continuity
- **OT/ICS Impact:** Minimal

Corrections Facility

- **Response:** SEVERELY LIMITED
  - Medical dispensing must continue
  - Door controls must remain operational
  - HVAC must function
- **Timeline:** Minutes to hours (lives at stake)
- **Concern:** Constitutional obligations
- **OT/ICS Impact:** CRITICAL

Cannabis Dispensary

- **Response:** Limited by banking restrictions
  - Cannot accept cards (cash-only)
  - HVAC controls must maintain climate
  - Cannot operate without tracking
- **Timeline:** Hours (license at risk)
- **Concern:** State compliance, crop integrity
- **OT/ICS Impact:** SEVERE

Law Firm

- **Response:** Constrained by ethics
  - Cannot disclose client matters
  - Cannot miss court deadlines
  - Cannot alert opposing counsel
- **Timeline:** Dependent on deadlines
- **Concern:** Attorney-client privilege
- **OT/ICS Impact:** Low

Municipal Recreation

- **Response:** Public sector constraints
  - Pool systems must continue
  - HVAC must maintain safety
  - Cannot afford commercial IR rates
- **Timeline:** Hours (health code violations)
- **Concern:** Public safety, compliance
- **OT/ICS Impact:** SIGNIFICANT

> **I don't believe umbrella ISACs can provide effective guidance for all these scenarios. The technical attack is identical, but in my experience, the contextual response requirements are so radically different that generic "ransomware response guidance" simply doesn't serve these sectors well. I've seen firsthand that each sector needs intelligence from people who deeply understand their operational reality, including which systems are OT/ICS, what those systems control, and what the real-world consequences are if they fail.**

When Specialization Works (Corrections Sector as an Example)

Real successes from OTICS-ISAC show what I believe is possible with specialized intelligence:

Contraband phone detection system vulnerabilities. Sector-specific intelligence helps corrections IT understand these aren't just network security issues. They have constitutional implications and require understanding inmate behavior patterns.

Door control system threats. Corrections-focused intelligence recognizes that these OT/ICS systems are fundamentally different from building access controls in corporate environments. Compromises can enable escapes or create safety emergencies requiring immediate lockdown.

HVAC system security. Specialized analysis shows how temperature control failures violate Eighth Amendment protections and how compromised systems can be used to create disturbances or mask other security breaches.

Visitation scheduling system threats. Sector knowledge reveals how schedule manipulation facilitates contraband smuggling and how compromised visitor databases create safety risks.

Body scanner security. Corrections-focused intelligence recognizes that exploits could allow weapons into facilities. The consequence isn't data loss; it's protecting lives.

Commissary system integrity. Sector knowledge reveals that financial fraud can fund gang activity and transaction manipulation can trigger facility disturbances.

This is intelligence you can actually use. It speaks the language of corrections professionals and addresses their real operational challenges.

The Resource Opportunity

Some argue that instead of investing resources to create new organizations, it would be more effective to better leverage existing structures.[1]

But I believe this perspective misses the real opportunity:

Underserved sectors aren't getting intelligence now. Creating specialized ISACs doesn't compete with existing ones. It serves communities that aren't currently protected.

The investment makes economic sense:

- Sector-specific ISAC: $500K to $2M annually
- Single ransomware attack on corrections: $10M to $50M
- Single cannabis crop failure from HVAC compromise: $2M to $10M

The ROI is compelling.

Specialized ISACs strengthen the entire ecosystem. When OTICS-ISAC identifies a corrections-specific threat, we share technical indicators through the National Council of ISACs. Everyone benefits from intelligence that wouldn't exist without sectoral specialization.

Sectors Ready for Their Own ISACs

Cannabis Industry

Context: Cash-based operations, federal-state conflicts, state tracking

OT/ICS: HVAC, irrigation, monitoring

Municipal Recreation

Context: Public access, limited budgets, minor PII

OT/ICS: Pool systems, HVAC, access controls

Legal Services

Context: Attorney-client privilege, court deadlines

OT/ICS: Minimal (IT-focused)

Hospitality/Tourism

Context: Guest privacy, PCI compliance

OT/ICS: Keycards, building automation

Agricultural Technology

Context: IoT sensors, autonomous equipment

OT/ICS: Tractors, irrigation, climate control

The Cross-Collaboration Imperative

Here's something critical that I believe often gets lost in these discussions: **Advocating for more specialized ISACs doesn't mean advocating for silos.** We need robust cross-sector collaboration capabilities precisely because threats don't respect sectoral boundaries.

The challenge isn't whether ISACs should collaborate; it's how they can effectively share intelligence when they're using different technologies and platforms. Today, one ISAC might be using MISP (Malware Information Sharing Platform) while another uses a proprietary commercial platform, and another relies on ThreatConnect or secure email lists.

I believe the solution isn't fewer ISACs; it's better interoperability. We need investment in universal standards for threat intelligence sharing, cross-platform integration capabilities, and perhaps a

backbone platform or hub that all ISACs can connect to regardless of their internal systems. Think of it like email: everyone uses different providers, but they all interoperate because they follow common protocols.

The National Council of ISACs is working on some of this, but in my view, we need accelerated investment. Specialized ISACs actually make this MORE important, not less. When you have deep sectoral expertise identifying nuanced threats, you create more valuable intelligence to share, but only if we have the technical infrastructure to share it effectively.

The Path Forward

I got that IT job because I understood that IT was too vast for anyone to master completely. I demonstrated the value of continuous learning, specialization, and staying current in my domain.

I believe the cybersecurity community can embrace the same principle.

> **There's widespread agreement that "sector-specific ISACs are well attuned to their members' needs and can tailor threat intelligence and mitigation practices accordingly."[1] Let's apply this insight to build new ISACs for underserved sectors.**

We can build a stronger defense ecosystem through specialization.

No one knows everything. Not in IT. Not in cybersecurity. And certainly not in threat intelligence.

We need more ISACs. More specialization. More sector-specific expertise.

Because the alternative (pretending that one ISAC can serve everyone effectively) misses the incredible strength that comes from deep sectoral knowledge.

The future of threat intelligence is specialized, community-driven, and built for the unique challenges each sector faces.

Let's build it together.

References & Sources

1. IT-ISAC. (August 2025). "Leverage Existing ISACs to Share AI Threat Information." https://www.it-isac.org/post/leverage-existing-isacs-to-share-ai-threat-information

About the Author

Ian Andriechack is CEO of **ALLITSystems LLC**, a cybersecurity company specializing in OSINT and threat intelligence. With nine years of corrections experience and 13 years of cybersecurity and IT experience, he operates the **Nexus Sentinel** OSINT platform and supports multiple ISACs including **OTICS-ISAC**.

The views expressed in this article are my own based on my experience supporting multiple ISACs and working in the cybersecurity field.

Connect With Us

OTICS-ISAC

ALLITSystems

Blog

Podcast

Nexus Sentinel

ShadowScan