

ISA CROSS SECTOR AI STUDY IDENTIFIES CONVERGENT NEEDS OF SECTORS

By Larry Clinton, President Internet Security Alliance

The Internet Security Alliance (ISA) is conducting a cross-sector assessment by critical infrastructure entitled “Defining an Effective and Sustainable Model for AI Deployment in Critical Infrastructure.” The study is based on reports of CISOs from five critical sectors – defense, energy, health, financial services and IT. The first phase of the study identifies security challenges and gaps identified by the CISOs related to AI adoption in these five critical sectors.

These posts will outline the results of the first two phases in ISA’s program. Full results of phases one and two in this study will be presented in a congressional briefing on September second.

In the first phase of the study CISOs identified the challenges and gaps they were already experiencing within their sectors. In the second phase the individual sector specific reports were fed into AI tools which identified eight specific areas wherein all five sectors noted virtually identical gaps and challenges.

These cross sectoral challenges and gaps point toward new areas of concern that policy makers may need to address. These areas of convergence also suggest the need to fundamentally rethink and reform the policy making process which currently is based on largely industrial age distinctions between sectors which AI may obliterate.

While sector specific distinctions will obviously remain, the speed and altered economics of the AI era will likely demand a more efficient and effective model for governance. A reformed model – a social contract – that takes into account both the expanded needs for security in privately owned critical infrastructure and the ongoing need for a market-based economy to sustainably provide services and innovative methods in an ever more competitive AI world,

Areas of convergence across the sectors

The five reviews were prepared separately by organizations that share no common threat model, regulator, or consequence profile. They converged on the following findings.

1. Adoption is outrunning governance in every sector, including at the most capable organizations. One sector reported that a mature, well-funded responsible-AI program with review boards and a unified deployment platform is still outpaced by its own adoption. Another reported four decades of sector AI use and concluded that its vulnerability doctrine, data boundaries, and assurance models were built for a different technology. The gap is structural, and additional maturity or budget alone will not close it.
2. Agentic AI presents a different governance problem from the AI these sectors have managed before. Earlier analytic and predictive systems produced output that a person then acted on. Agentic systems plan and execute actions themselves, using credentials, tools, and connections to other systems. They function as participants in operations rather than as features within applications, and the governance disciplines built for software and for human users do not fully apply to either.
3. The risk sits primarily in the operating envelope around the model rather than in the model itself. What matters operationally is identity, permissions, tool access, data connections, monitoring, and lifecycle. This is a constructive finding, since most of the needed controls are extensions of disciplines these organizations already run, applied to a new category of actor.
4. Periodic compliance no longer describes the systems being governed. All five sectors reported that annual assessment and static certification cannot ensure that systems retrain, acquire new tools, and change behavior continuously between reviews.
5. The timing of defense has inverted. Attackers now operate at a speed human review cycles cannot match. In sectors with physical operations, containment options remain coarse, so isolating a compromised component often means interrupting service.
6. The threat is industrialized rather than exotic. The dominant concerns are fraud at scale, synthetic identity, convincing impersonation, manipulation of training data, and compromise through third parties. These are current operational realities, not speculative future capabilities.
7. Smaller entities in every sector cannot carry this burden alone, and several perform functions of national consequence. Community financial institutions, rural and safety-net providers, mid-sized utilities, and small cleared defense suppliers face the same adversaries with a fraction of the staff and capital.

8. All five sectors prefer risk-tiered, incentive-based approaches to uniform prescriptive mandates, and all five hold that accountability belongs at the board level and must rest on evidence rather than assurances.

The sectors diverge on consequence rather than diagnosis. Failure is a physical safety and service continuity problem in energy, a classification and national security problem in the defense industrial base, a systemic confidence problem in financial services, and a patient safety and access problem in healthcare. Information technology is distinctive because its members are frequently the shared dependency on which the other four rely.

Coming next: Specific gaps that must be filled