You Can Feel It. You Can’t Name It Yet.

The country’s most consequential operators are being called into an alliance around a problem coordination can only half solve.

THOMAS ROCHA III

AUG 06, 2026

On August 5, Reuters reported that Jamie Dimon and the Alliance for Critical Infrastructure had approached more than forty companies across banking, technology, energy, water, utilities, telecommunications, airlines, and railroads to expand the group and sharpen its focus on AI risk. Dimon personally contacted the CEOs of major banks and

technology firms. The purpose, as reported: share intelligence, develop common safeguards, coordinate with the government. The results of the outreach have not been disclosed, and the revamped alliance is meant to be fully operational by year-end.

Read that as what it is. The people who operate the most sophisticated infrastructure on earth have looked at what happens when AI agents begin acting across their systems, and they have judged the danger large enough, and shared enough, that meeting it requires organizing across industry lines. Not within one company. Across all of them.

They are right that it is shared. They are right to organize. And the thing they are building addresses half of the problem, because half is the part you can share.

What you can share, and what you can't

You can share what you know. That is what an alliance is for. One operator sees a new attack, a new failure mode, a new way an agent goes wrong, and tells the others. Threat intelligence pools. Everyone gets smarter at the same rate. This is real and it matters and it is exactly the right response to a shared risk.

You cannot share authority the same way.

Now follow the structural condition one level deeper than the alliance's stated concern. As AI-assisted operations begin crossing independently controlled systems, they run into a class of risk that information sharing alone cannot reach. Picture the chain: a bank or utility employee starts an action, an enterprise agent picks it up, an outside model processes it, it crosses a telecom network, runs through a cloud service, and reaches an infrastructure operator who executes something consequential. A payment clears. A grid setting changes. A valve opens.

Every company in that chain can share what it learned about the threat. What none of them can pool is the answer to the question that governs

whether the action should have happened: at this moment, in this operation, is the actor requesting this step actually authorized to cause it, on whose behalf, and does that authority still hold now that the operation has crossed out of the system that granted it?

A downstream system may verify a credential, a signed instruction, a token, a policy decision. That verification does not by itself prove that the authority governing the operation remained valid as the operation changed state, system, context, and control domain. The credential checks out locally. Whether the authority behind it survived the crossing is a different question, and no participant in the chain is positioned to answer it, because each granted, or received, only its own piece. None governs the whole live act as it moves.

That is the half the alliance cannot solve by sharing, because it is not a knowledge problem. It is a runtime problem. And it does not only live in power grids.

The same seam, one floor down

Strip the stakes away and look at an ordinary business. Any business.

It runs one continuous customer interaction: marketing, advertising, sales, shopping, buying, delivery, service, support. To the customer it is one relationship. Inside the company it is a relay of separate systems, each owned by a different team, often a different vendor, each measuring itself by the one thing it can count. Marketing counts impressions. Advertising counts clicks. Sales counts leads. Shopping counts carts. Buying counts conversions. Delivery counts on-time rates. Service counts tickets.

Every number is real. Every system works. And between every two of them is a handoff, the place where the customer, and everything true about them, passes from one system to the next.

That handoff is the seam. It is the same structural seam now becoming visible in critical infrastructure: the transition between independently controlled systems, where local controls stop and no continuous authority governs the crossing. One floor down, and a thousand times a day.

The failures are not identical. A cyberattack on a grid, a broken consent handoff, and a price that changes between the ad and the checkout are different problems with different consequences. What is identical is the structural condition underneath them: fragmented control domains, a live operation crossing between them, each system validating only its own local state, and no continuous authority context remaining provable across the whole transition.

At the seam, the authority governing what just happened must remain bound to what happens next. Usually, it does not. And authority here does not mean rank or a static permission. It means the conditions under which an act, a promise, a consent, or a decision may become binding, and who has the standing to make it so. The promise marketing made has to bind what sales can honor. The consent the shopping tool captured has to bind what the service desk may later do. The price advertising displayed has to bind what checkout charges. For years a person stood at each of those seams and carried that authority across by hand. The rep who knew what was promised. The manager who approved the exception. The human who remembered.

Automation removed the humans and kept the seams.

The interaction still flows across them. The authority governing it falls out at every one. And almost nobody can see it happening, because each system reports that it is working, and each system is telling the truth about itself.

Why you can feel it before you can name it

You have felt this. You may not have had a word for it.

It is the revenue that leaks somewhere between the ad and the sale and never shows up in any single system's numbers, because each system hit its own target. It is the liability that lands on you from a vendor's tool you do not operate, over a claim you never saw made. It is the customer who was told one thing and charged another, and when you go looking for who authorized the difference, there is no one, because the promise crossed a seam where no authority was carried and became an orphan, a thing the customer was told that no one in the building ever stood behind.

You feel it as friction, leakage, surprise exposure, deals that die in the handoff, customers who fall through. What you are feeling is always the same thing in a different costume. The authority did not survive the crossing.

The reason it stays nameless is that no part of your stack is responsible for the space between the parts. Each system governs itself and reports itself as working. None governs whether a given act stayed authorized as the interaction moved from system to system, hand to hand, company to company. The seam belongs to no one, so the failure at the seam has no owner and no name.

The thing you have been paying for

So name it plainly.

Businesses have built controls inside each system: identity, access, workflow, consent capture, policy enforcement, audit. What they have generally not built is a continuous authority layer spanning the transitions between those systems. That layer went unbuilt because, until recently, a human was standing in it. Its job is to keep the governing authority and its conditions continuously bound to an interaction as that interaction crosses systems, teams, vendors, and organizations, and to make sure that when something consequential happens, it can be shown to have been authorized by someone with the

standing to authorize it, under conditions that still held at the moment it occurred.

It is not reducible to identity, access control, security policy, compliance, logging, or workflow. Each supplies part of the answer. None by itself establishes whether this particular act may become binding, on whose authority, under conditions that still hold as the interaction changes.

Most businesses still have no name for this layer. I have been describing it, and the architecture that governs it, since 2024. What is new is that the problem is now surfacing independently across the technical world. In the space of a few months in 2026, separate research groups began formalizing exactly this requirement, causal authority propagation that never widens as it crosses steps, authority modeled as derived state rather than standing permission, proofs that an action was authorized by the lineage that caused it, fail-closed when it cannot be shown. Different teams, different labs, no coordination, arriving at the same primitive from different sides. That is not noise. It is what happens when a real architectural category becomes unavoidable: everyone who hits it starts reaching for the same shape, and eventually the same words.

Call the category authority continuity, or, more precisely, runtime authority continuity: keeping the governing authority and its conditions bound to an interaction as that interaction changes systems, states, vendors, and organizations. Not a product, not a feature. A distinct layer of the business, and at the moment it is rarely governed as a distinct, continuous layer, because the humans who used to govern it by presence have been automated out of the seams they were standing in.

I have written about the underlying principle elsewhere, as authority that survives mutation, and the architecture that carries it. This piece is not about that architecture. It is about the fact that the layer exists, that it is rarely owned as a distinct layer, and that you have already been paying for its absence without a line item to put it on.

This already happened

Notice the tense. None of this is a forecast.

The systems are already fragmented. The humans have already left the seams. The value is already leaking through them, and the liability is already arriving through them, and Jamie Dimon and the ACI are already recruiting from more than forty of the country's most consequential companies because the most exposed operators can feel it too. They have reached the size of exposure where feeling it is no longer survivable, so they are organizing.

That is the tell. When the banks and the grids and the telecoms start forming a coalition around a problem, the problem is not coming. It is here. They will share what they know, and they should. But the part they cannot share, the authority over the live act as it crosses from one hand to the next, is the same part quietly draining every ordinary business that ever automated a handoff and assumed the promise would carry itself across.

You could feel it before you could name it. Now you have a name for it, runtime authority continuity, and a place to look for its failure: the seams, where nobody is standing anymore.

The only question left is whether you can see them now.