Written Input to the SEC Crypto Task Force

Submitter: Jing Jian, Founder, Inherence Labs **Date:** June 2026 **Re:** Conduct-level proof: privacy-preserving verification of mandate adherence for autonomous and on-chain market activity

To Commissioner Peirce and the members of the Crypto Task Force:

Thank you for the opportunity to provide written input, and for the December 15, 2025 roundtable on financial surveillance and privacy. Inherence Labs is a small, early-stage company of the kind the Task Force solicited during its 2025 outreach. We build technology, implemented and working today, that turns the rules an automated actor must follow into both runtime enforcement and a zero-knowledge proof of adherence. This letter identifies a gap in the compliance architecture taking shape in the public record, offers a definition and functional criteria the Commission may find useful, and closes with an offer to demonstrate the capability to the staff.

Disclosure. Inherence Labs holds pending patent filings on one implementation of the capability described herein. The definition and criteria proposed below are functional and technology-neutral, and would apply equally to any qualifying approach by any implementer. This input is submitted to support the Commission's stated goals of investor protection and privacy-preserving compliance.

1. Three layers of compliance are forming, and one is missing

The December roundtable established the principle. Chair Atkins observed that privacy-preserving tools can let users prove compliance without handing over their entire financial history, and that institutions depend on the ability to build positions and test strategies without telegraphing that activity to competitors. Commissioner Peirce observed that zero-knowledge proofs can show that someone is permitted to conduct a given transaction while shielding private information.

The written record since then is best understood as three layers, each answering a different question.

Attribute-level proof answers who may act. Identity and accreditation credentials, and a recent meeting memorandum describing cryptographic proof of jurisdictional presence at the moment of a transaction, sit here.

Asset-level enforcement answers what an asset permits. An April 2026 petition for rulemaking proposing recognition of persistent-enforcement systems, in which conditions ride on the asset and are enforced automatically across transfers and platforms, sits here.

Conduct-level adherence answers what the actor actually did. We propose the following definition: *conduct-level adherence is whether an actor's entire sequence of actions complied with the mandate governing it, where a mandate includes both rules that bind each individual action and rules that accumulate across actions, such as budgets, exposure limits, and exclusions.*

The first two layers are valuable and well represented in the record. We have not found a submission that addresses the third. Yet the third is the layer that determines investor protection once activity becomes autonomous: whether an automated strategy stayed within its stated investment limits, whether an AI agent stayed within its authorized budget and scope, and whether quantitative bounds held at every step and across the entire sequence of actions.

2. Why conduct-level proof becomes necessary

Traditional oversight rests on three conditions: time to review activity before damage compounds, the ability to reverse mistaken transfers, and known counterparties subject to reputation and regulation. Autonomous on-chain activity removes all three at once. Transactions are instant, settlement is final, and the counterparty may be software. Periodic, after-the-fact examination is structurally mismatched to conduct that occurs at machine speed and cannot be unwound. Verification must move to the moment of action.

The gap is no longer hypothetical. In recent federal litigation between Amazon and Perplexity concerning an AI shopping agent, the court distinguished actions taken with a user's permission from actions authorized by the platform on which the agent acted. Because no instrument existed by which the agent's conduct could be independently demonstrated, the parties' only available tools were technical blocking and litigation. As agents proliferate, that is not a scalable model of trust for markets.

The December record also identifies why disclosure-based demonstration fails here. Full transparency exposes strategies and positions, which disincentivizes legitimate market activity, as the Chair noted. Conduct-level compliance therefore requires demonstration without disclosure.

A related structural point concerns consolidated platforms. Where a single operator provides custody, execution, and oversight, the separation between parties that traditionally produced independent verification is absent, and the operator's own records are the only evidence of its own compliance. The April 2026 petition states correctly that verification of ownership is not

enforcement of conditions. We respectfully add the complement: enforcement is not proof. An enforcement mechanism whose operation cannot be independently verified asks clients, counterparties, and the Commission to trust the operator's word.

3. The technical capability exists

We wish to place on the record that the following is practical today and implemented in working software. A mandate, meaning the full set of rules an automated strategy or AI agent must follow, including quantitative limits maintained across sequences of actions, can be compiled into two artifacts from a single specification: a runtime enforcement component that evaluates each proposed action before it executes, and a zero-knowledge proof that the action, and the sequence of actions as a whole, adhered to the mandate. Because both artifacts derive from one specification, the enforcement and the proof cannot diverge. The proof is succinct, can be checked by any party without access to the operator's systems, and reveals nothing beyond adherence itself: neither positions, nor counterparties, nor the contents of the mandate. The cost of extending coverage is constant for each additional action, so the approach scales to long-running activity without a growing proving or verification burden, and it operates at the speed of live markets. The method is the subject of pending patent applications. We would welcome the opportunity to demonstrate it to the staff, and Appendix A provides a brief illustration.

4. The surveillance concern deserves a structural answer

A written statement submitted in connection with the December roundtable cautioned that voluntary cryptographic attestation could harden into a mandatory disclosure regime, and that compliance infrastructure can make surveillance frictionless. The concern is legitimate and should shape the Commission's approach. Conduct-level proof, correctly specified, answers it structurally: the verifier learns a single fact, that the mandate was followed, and nothing else. The underlying data never moves. Compared with disclosure-based compliance, in which records flow to intermediaries and authorities and accumulate, proof-based compliance reduces the information that leaves the regulated firm. The same property aligns with data-minimization principles that other jurisdictions are increasingly treating as mandatory in their anti-money-laundering and data-protection regimes. The criteria below are drafted to preserve that property, and we agree that such mechanisms should remain voluntary means of satisfying existing obligations and should not become new mandates.

5. Recommendations

We recommend that the Commission, in guidance or rulemaking arising from Project Crypto:

1. Treat independent verifiability as a requirement distinct from enforcement in any framework addressing automated or persistent-enforcement systems. Enforcement determines what can occur. Verification determines what others can know occurred. Investor protection in autonomous markets requires both.
2. Define functional, technology-neutral criteria for acceptable compliance demonstrations: (a) independently verifiable by a third party without access to, or trust in, the operator's systems; (b) tamper-evident; (c) continuous, covering each action and the sequence of actions as a whole; and (d) privacy-preserving, revealing no information beyond the fact of adherence.
3. Permit regulated firms to satisfy appropriate demonstration obligations with cryptographic proofs meeting those criteria, including adherence of automated strategies to their stated mandates and limits, where the proof provides equal or greater assurance than disclosure-based alternatives, consistent with Regulation S-P.
4. Recognize conduct-level adherence, as defined in Section 1, as a distinct compliance object alongside attribute-level eligibility and asset-level conditions when evaluating frameworks for AI-driven and autonomous transactions.

6. Closing

Inherence Labs is available to meet with the Task Force, to demonstrate the working system, and to respond to questions from the staff. Thank you for the Task Force's sustained engagement and for the opportunity to contribute to the record.

Respectfully submitted,

Jing Jian
Founder, Inherence Labs
Los Angeles, California

Appendix A: An illustration of conduct-level adherence

Scenario. A client delegates trading to an automated agent under a mandate: a total budget of $50,000; no single position exceeding 10 percent of the portfolio; no leverage; a list of excluded assets. Over one week the agent executes four hundred actions.

What existing instruments establish. A signed record shows the client authorized the delegation. Identity attestation shows which agent acted on each request. Settlement records show each payment cleared. Point-in-time compliance checks show each transaction individually passed at the moment it occurred. All of these are necessary, and all are snapshots. Whether the 10 percent cap held as positions accumulated across the week, whether cumulative

spending stayed within the budget, and whether the exclusions held in every combination can be established today only in two ways: by trusting the operator's own records, or by disclosing the complete trading history for inspection.

What conduct-level proof establishes. Each proposed action is checked against the compiled mandate before it executes, so non-compliant actions do not occur. At any point in the week, the agent's operator can produce one compact proof that the entire sequence adhered to the mandate. The client, a counterparty, or an examiner can verify that proof without access to the operator's systems and without learning the positions, the strategy, or the mandate's terms. The verifier learns one fact: the rules were followed.

Mapping to the criteria in Section 5. The proof is checkable by any third party (independently verifiable); it cannot be altered without detection (tamper-evident); it covers every action and the week as a whole (continuous); and it discloses nothing beyond adherence (privacy-preserving).