MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Phylax Systems, Inc.

On June 2, 2026, Crypto Task Force Staff met with representatives from Phylax Systems, Inc.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Phylax Systems, Inc. representatives provided the attached document, which was discussed during the meeting.

Phylax Systems Attendees:

1. Odyssefs Lamtzidis: Founder & CEO
2. Cindy Chau, Product & Strategy

---

1. Overview of the Current State of DeFi Security

Estimated time: 10 minutes

We will begin with a brief overview of the current DeFi security landscape. Despite major advances in smart contract development, formal verification, and third-party audits, protocol failures and exploits continue to occur. In DeFi, security incidents are not isolated software bugs; they are “physics events”. Impossible to retroactively fix, in contrast with traditional finance. The same attribute that enables the unprecedented capital efficiency – instant settlement – is also what makes security incidents extremely destructive.

2. Why Current Security Models Often Depend on Centralized Control

Estimated time: 10 minutes

Many DeFi protocols currently rely on emergency controls such as admin keys, security councils, guardian roles, or multisignature wallets. These mechanisms are often introduced for understandable reasons: to stop attacks, pause markets, upgrade contracts, or respond to unforeseen risks. However, they also create governance and regulatory tradeoffs.

In practice, emergency response systems may require humans to identify an attack, coordinate across signers, and act quickly under uncertainty. This can be too slow during an active exploit, and it can also concentrate discretionary power in a small group of individuals or entities. Security councils may be necessary in some cases, but they can also make protocols look and operate more like centrally managed systems.

We would like to discuss this tension directly: policymakers are understandably focused on the degree of centralization in crypto systems, but some security practices intended to protect users may themselves introduce centralizing features. The question is whether protocols can achieve strong safety guarantees without relying on unilateral human control.

3. Phylax's Approach to Decentralized DeFi Security

Estimated time: 15 minutes

Phylax is developing a different approach to DeFi security. Rather than assuming protocols can write perfect code or enumerate every possible attack in advance, protocols can define unacceptable economic outcomes and prevent those outcomes from occurring.

For example, a protocol may define conditions under which a market should not allow further withdrawals, borrowing, liquidation, minting, or other sensitive actions. These conditions can be monitored transparently and enforced automatically, without requiring an administrator or multisig to make a discretionary intervention after the fact.

Effectively, we are expanding the set of constraints developers can express, enabling them to identify and prevent failure scenarios that before would be impossible to express.

The goal is to create an instant, autonomous circuit breaker and safety net for smart contracts. This type of system can help contain catastrophic losses, reduce contagion risk, and give users and regulators clearer visibility into how risk controls operate. Importantly, the model is designed not to introduce new centralized control. The protections can be transparent, auditable, and rule-based, with enforcement tied to predefined conditions rather than arbitrary human decisions.

4. Demo: What Decentralized Safety Looks Like in Practice

Estimated time: 15 minutes

We will provide a practical demonstration of how circuit-breaker-like protections can operate without an admin key. The demo will show how a protocol can monitor for dangerous states and trigger predefined mitigations automatically, without giving any single operator unilateral control over user funds or protocol logic.

The demonstration will cover three themes:

First, how catastrophic exploit containment can work in real time. The objective is not to reverse every bad outcome after an incident, but to prevent an attack from cascading across the system once predefined risk thresholds are crossed.

Second, the evidence layer that is provided as part of the system and provides both the protocols, as also the community and regulators with the transparency and auditability that one expects from blockchain systems.

Third, how governance can define the safety framework without becoming an emergency operator. This distinction is important: governance may set risk parameters and approve safety logic in advance, while the system itself executes according to those rules when specific conditions are met.

We will also discuss how these designs can support policy goals such as market integrity, investor protection, and credible compliance incentives where relevant, while avoiding design requirements that unintentionally force DeFi protocols to become centralized intermediaries.

5. Regulatory Discussion and Potential Disclosure Frameworks

Estimated time: 7 minutes

We would like to discuss how security expectations for smart-contract-based financial systems could be framed in a way that improves user protection without mandating centralized control.

One possible area for consideration is transparent security attestations as part of disclosures for smart contract systems. These attestations could describe the protocol's security assumptions, audit history, emergency controls, automated safety mechanisms, upgrade authority, governance process, and known limitations. The goal would not be to guarantee that a protocol is risk-free, but to give users, market participants, and regulators a clearer view of how the protocol handles foreseeable failure modes.

We believe that the industry has made great strides in identifying and surfacing the financial risk of the various protocols or investment vehicles, but failed to do so when it comes to counter-party risk. The recent events with KelpDAO, LayerZero, and AAVE showcase not only how the risks were ignored by multiple parties, but also how an isolated incident turned into a systemic event.

This could help distinguish between systems that rely on opaque discretionary intervention and systems that use transparent, auditable, precommitted controls. It may also help avoid a regulatory outcome where protocols are pushed toward centralized admin structures simply because those are the most familiar form of emergency response.

6. Key Takeaway

Estimated time: 3 minutes

The core message is that DeFi security does not have to depend on shortcuts such as trusted admin keys, ad hoc intervention, or the hope that audits will catch every possible failure. Smart contract systems can be designed with transparent, autonomous, and decentralized safety

mechanisms that prevent unacceptable outcomes before they destabilize users, markets, or tokenized financial infrastructure.

It does not have to be this way. We can secure smart contracts without collapsing them into centralized systems. We can reduce the risk that a single hack destabilizes broader tokenized finance.