April 16, 2025

by electronic submission

Commissioner Hester M. Peirce
Chair of SEC Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549

RE: RECOMMENDATIONS REGARDING INDEPENDENT SECURITY AUDIT REPORTS

Dear Commissioner Peirce and Members of the SEC Crypto Task Force,

OpenZeppelin appreciates the opportunity to provide written recommendations regarding the disclosure obligations and other requirements that could be applied to crypto assets and their related blockchain applications ("**Protocols**") and those market participants that may interact with Protocols (e.g. exchanges, custodians, broker-dealers and investment managers) that are subject to the federal securities laws (even if for a limited period of time, for example pursuant to a safe harbor framework). We welcome opportunities to meet with Securities and Exchange Commission staff, answer any questions that the Commission may have, and discuss our recommendations below in more detail.

OpenZeppelin has provided a range of specialized cybersecurity solutions to the blockchain industry for almost 10 years, partnering with clients ranging from startups to Fortune 500 companies, including major financial institutions and intermediaries. Over $20 trillion in value has been transferred via OpenZeppelin's open-source smart contracts and our firm pioneered the security audit practice, which has become a *de facto* best practice in the industry. Prior submissions to the Crypto Task Force have highlighted the importance of cybersecurity and related audits. Additionally, the Commission's Division of Corporation Finance recently cited the relevance of third-party security audits in its "Offerings and Registrations of Securities in the Crypto Asset Markets" guidance.

We believe that any regulatory regime applied to Protocols should promote cybersecurity best practices by requiring a third-party security audit, which can ensure that the promises of blockchain technology are ultimately realized in the United States. When developed and operated securely, blockchain applications present significant advantages when compared to "web2" applications. This is because blockchain applications can guarantee users access, availability and integrity in accordance with their encoded rules, without being subject to the

multitude of risks and costs that arise when users have to rely on centralized technology or service providers.

The primary aim of a third-party security audit is to critically assess a Protocol's code and evaluate if the Protocol is expected to operate in accordance with its documentation and stated purpose (e.g., token utility and supply, transfer restrictions, blockchain fees, etc). Given the risks of centralized points of failure, particular attention is paid by auditors to the upgradeability and governance of such code (e.g., who can access and control functions). Audit reports note any discrepancies or issues identified, as well as include an evaluation of compliance with broader security standards that can help a Protocol reduce the likelihood of issues arising in the future.

The lack of clear requirements mandating high-quality Protocol security audits has resulted in too many examples of Protocols that have failed to operate in accordance with the expectations of their developers and users alike, with issues and exploits leading to significant losses of capital and consumer confidence. The history of software development in other critical industries (e.g., healthcare, aerospace, etc) has shown that when developers are incentivized to follow, document and maintain security best practices, it results in secure applications that users can trust. Therefore, we recommend that the Commission consider implementing some or all of our recommendations included in this letter (including the details regarding security audits set forth in Exhibit A below) in order to ensure the United States emerges as the global leader in blockchain technology. We believe this would support the Commission's mission to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.

Our recommendations are informed by our long-standing relationships with leading Protocols who have already adopted security best practices on a voluntary basis. These Protocols have built trust through their strong track record and transparency regarding their security posture, including by regularly conducting and publishing security audit reports conducted by specialized audit firms like OpenZeppelin. A regulatory requirement to conduct audits could formalize such industry best practices and help root out those that seek to take shortcuts and put all market participants at risk.

We believe adoption of these recommendations by the Commission could also prove pivotal to the broader discussion surrounding the regulation of Protocols that are not securities, whether through statutory efforts or otherwise. Given that security audit reports provide independent disclosure regarding the operation of a Protocol and related risks, they can also be used to meet other regulatory goals. We look forward to engaging constructively with all interested stakeholders.

Sincerely,

John Neufeld
General Counsel
OpenZeppelin

EXHIBIT A

PROPOSED SECURITY REQUIREMENTS
AND RELATED AUDIT METHODOLOGY

Security Requirements

Not all requirements will be applicable to all Protocols. An Audit Report (as defined below) could note that a requirement is met, potentially with contextual information regarding how it is met, or with a reference to relevant Protocol materials (e.g., a hyperlink to an official website, documentation or "trust center"). Similarly, a note could be made where a requirement is not applicable or practicable.

Audit Reports for a given Protocol should not cover applications offered by third parties that a user may choose to utilize to interact with such Protocol (e.g. wallets, certain front-end interfaces, etc). It is likely that such third-party service providers build trust through another method (e.g. SOC 2 or ISO 27001) or would be subject to these security requirements themselves.

- **Development**
    - **Open-source Libraries:** the Protocol inherits the security assurances of audited, open-source libraries that have proven secure over time and novel code is only utilized where necessary.
    - **Documentation**
        - **System Overview:** the Protocol is accompanied by robust documentation that accurately describes its functionality, its economic model, its components (both internal and external), the expected level of service, the risks associated with its use, the responsibilities of the various stakeholders, and the governance mechanisms involved.
        - **Technical Documentation:** the Protocol's source code includes a Readme file, docstrings (e.g., in NatSpec format), and inline comments.
        - **Address Book:** the Protocol documentation includes an "address book" that includes the addresses of all smart contracts (or similar) included in the current version of the Protocol, including links to such smart contracts on a public block explorer for the relevant blockchain network(s). Other Protocol-specific guidance to minimize risks targeting users is encouraged.
    - **Testing:** the Protocol code base has comprehensive test coverage, which can be accessed together with the Protocol source code (see below). Testing may vary depending on the nature of the Protocol and its components, however key invariants should be defined in the documentation and appropriate testing must be performed and passed (e.g., static analysis, dynamic analysis or formal verification).

    - **Code Audits:** all blockchain and smart contract (or similar) code must have undergone a manual, human review (preferably by at least two code auditors reviewing all in-scope code line-by-line) by a Qualified Auditor (defined below) to identify any known or novel vulnerabilities. Further:
        - **Scope:** code audits must have a broad enough scope for a Qualified Auditor to agree to issue a public code audit following its ordinary procedures. If appropriate, code already audited by any Qualified Auditor may be considered secure under a trust assumption and removed from scope (including unmodified code from an established open-source library subject to an appropriate security program).
        - **Automated Tools:** the use of automated tools to identify vulnerabilities is encouraged, however it may not be used as a substitute for manual review.
- **Deployment**
    - **Compilation:** the compilation of the Protocol's source code is deterministic and can be reproduced without error and addresses any compiler issues.
    - **Verified Bytecode:** the Protocol bytecode deployed to any blockchain network(s) is verified as corresponding to the source code that was subject to a code audit by a Qualified Auditor. Such verification is publicly available, for example through a block explorer.
- **Operations**
    - **Source Code:** the Protocol source code must be published publicly, to ensure transparency of the service provided and enable responsible bug disclosure and patching.
    - **Security Contact:** the Protocol must appoint a designated security contact with sufficient skills and experience to manage any potential security issues. Confidential methods for contacting the security contact should be set out in documentation (e.g., in the NatSpec for EVM smart contracts).
    - **Monitoring:** those charged with security of the Protocol shall conduct regular risk assessments and threat modelling and implement real-time monitoring of such risks. Monitoring may trigger automated actions or incident response processes.
    - **Transaction Screening:** depending on the nature of a Protocol, it may wish to implement dynamic transaction screening on some or all activity to permit only certain pre-defined types of activity, or to block transactions that are flagged as malicious (for example, by simulating transactions before they are executed to determine if they present security or regulatory risks).
    - **Information Sharing**: those charged with security of the Protocol shall subscribe to and integrate industry-specific security information sharing tools (e.g. maintain memberships in industry-specific security information sharing organizations like ISACs).
    - **Bug Bounty Program:** a bug bounty program is operated for the Protocol with sufficient incentives for responsible disclosure of bugs in line with the Protocol's risk tolerance (e.g. which could be informed by value or impact).

    - **Incident Response:** those charged with security of the Protocol shall implement an incident response plan to guide the Protocol's response to any security incidents, which should at a minimum include a process to triage and remediate reported vulnerabilities based on severity and a communication plan to keep relevant stakeholders informed. The incident response plan should be tested and updated regularly (on at least an annual basis).
- **Governance**
    - **Documentation:** The processes of making and implementing decisions in relation to the Protocol are clearly and accurately described in public documentation, and any changes are updated without delay. To the extent feasible, voting power and constituents are identified and kept up to date programmatically.
    - **Upgrades and Timelock:** Governance arrangements shall include rules that safeguard the interests of users in the event of a change in the Protocol (such as provision of information regarding Protocol changes in advance, possibility of exit during a "timelock" that delays Protocol changes for a certain period of time, etc).
    - **Privileged Roles:** privileged roles, if any, are strictly limited to those necessary for proper performance of the Protocol and are clearly documented and highlighted as trust assumptions and secured using traditional security methods. In particular:
        - Any off-chain technology components or individuals or entities that have privileges to interact with the Protocol (there may be none in the case of "on-chain governance"), whether through a multi-signature wallet or otherwise, must be identified and implement comprehensive security and compliance standards (e.g., SOC 2, ISO 27001, or relevant blockchain-specific security standards).
        - Governance of a Protocol may include contingency mechanisms to ensure prompt responses to attacks or vulnerabilities. Safeguards accompanying such exceptional measures must be implemented (e.g., a list of activation events, possible actions, multi-step approvals) in order to limit the effects of Protocol disruption and to avoid the centralization risks of actors responsible for temporarily protecting the Protocol.

Audit Methodology

A valid security audit report produced by a Qualified Auditor (as defined below), which would express the Qualified Auditor's opinion about the Protocol's compliance with some or all of the security requirements set forth above (an "**Audit Report**") should be made available by a Protocol or other entity offering services related to a Protocol (e.g. exchanges, custodians, broker-dealers and investment managers). In particular, an Audit Report could note the procedures carried out by the Qualified Auditor in order to reach its conclusion and include any material deviations from the security requirements. Audit Reports could be written in "plain English" for a general audience.

An Audit Report could remain valid until the earliest of:

- any material update to the Protocol (for example, in the case of a decentralized application and/or its related crypto asset, any smart contract (or equivalent) upgrades, but not necessarily a smart contract parameter change);
- any material updates to the blockchain (if the Protocol is a blockchain), or the blockchain on which a Protocol operates; or
- 12 months following its evaluation date.

Although the current audit practice for blockchain technology is quite mature, specialized audit firms could additionally seek to form a dedicated non-profit organization similar to auditors in other fields (e.g. like those auditors that conduct SOC 2 or ISO 27001 reports). Such an organization could formalize current auditing standards in the blockchain space, set ethics requirements and manage accreditation to certify qualified auditors ("**Qualified Auditors**").

Given that security best practices transcend borders, it is likely that a single global organization would be sufficient for such purpose. Such an international organization could prove important in order to harmonize the evolving regulatory approaches concerning Protocols around the world, some of which will soon require the security best practices set forth herein. For example, see the requirements of the EU Cyber Resilience Act that is expected to come into force in 2027, in addition to the report of the working group of the AMF and ACPR and related proposals for the regulation of "DeFi" in the European Union through security certification.