Global Blockchain Business Council (GBBC) USA: Written Input to the U.S. SEC Crypto Task Force

GBBC USA welcomes the opportunity to provide written input to the U.S. SEC Crypto Task Force. We greatly value the SEC's ongoing engagement with industry stakeholders and its commitment to advancing a regulatory framework for digital assets that is clear, proportionate, and supports innovation.

This submission reflects Phase 1 of the consolidated effort of GBBC's Capital Markets Risk Mitigation Framework (RMF) Working Group, developed in consultation with a sub-set of a broad cross-section of GBBC's 500+ institutional members. Contributors include regulated financial institutions, global market infrastructures, blockchain protocols, technology providers, legal advisors, strategic consulting firms, and other participants from GBBC's international network.

Phase 1 RMF (working draft released on July 23, 2025, with consultation closed on October 3, 2025) provides a structured, technology-neutral framework for identifying and mitigating non-financial risks in blockchain infrastructures with a particular focus on public blockchains when deployed in regulated financial markets and digital assets securities. It addresses risk domains such as: Technology, Information Security & Cyber, Financial Crime, Third-Party Risk, Business Continuity, Legal, Data Management, Transaction Execution, Process Management, Conduct, Compliance, People & others.

RMF is directly relevant to Questions 21, 22, 40, and 45 that reference risks in custody arrangements and tokenization in the SEC's questionnaire under the Statement "There Must Be Some Way Out of Here." As we advance RMF Phase 2 and Phase 3, we will submit supplemental materials that continue to address the remaining questions and provide implementation guidance.

The regulatory landscape should be supporting principles-based standards rooted in practical risk mitigation and operational resilience ensuring all digital assets, including protocol tokens, can be safely custodied across diverse use cases and regulatory classifications. There is a critical opportunity to modernize the custody rules to enable the industry to adopt custody solutions that are technologically appropriate, while maintaining investor protection.

As highlighted in the RMF, digital assets introduce novel non-financial risks specific to public blockchain technology which necessitate targeted regulatory frameworks and mitigation strategies distinct from traditional asset custody. Custodians must also address fork handling, and technical coordination with protocol issuers or control agents, they are also ideal for facilitating cross-chain interoperability. Protocol token custody must incorporate robust security protocols, clearly defined

roles and responsibilities, and pre-authorized emergency mechanisms (e.g., circuit-breakers, reissuance procedures).

The Commission should treat the custody of digital assets in decentralized markets differently from that of traditional markets, given the distinct technical and operational features such as private key management, smart contracts, and programmable ownership, which introduce novel technology and legal risks. Traditional custody models reliant on centralized intermediaries are not suited for the decentralized nature of the digital assets market. A tailored regulation framework should recognize these realities, including additional security features such as multi-signature and MPC custody, the role of third-party validators, and the unique oversight challenges of self-custody, when "custody" means direct access to or control over private keys, making digital assets custody a fundamentally different paradigm.

Entities permitted to custody digital assets on behalf of clients may include both traditional financial institutions and crypto-native firms, provided they meet clear, risk-based standards for safeguarding client assets and are subject to appropriate regulatory oversight. Federally regulated banks and trust companies, as well as SEC-registered broker-dealers and CFTC-regulated entities such as FCMs and DCOs, already operate under established custody, segregation, and risk management frameworks and should continue to serve in this role – so long as they implement technologically appropriate key management and resilience practices rather than relying on legacy custody architectures. In addition, state-chartered trust companies have developed expertise and infrastructure tailored to blockchain-based custody and should be eligible custodians, subject to capital, cybersecurity, and audit requirements.

Custody of digital assets should be grounded in institutional-grade expertise in blockchain technology, cryptographic key management, and cybersecurity, supported by robust operational resilience and contingency planning. Regulatory standards should require secure cryptographic key management - such as Hardware Security Modules (HSMs), multi-signature schemes, and dual-control access along with secure peer communication, continuous monitoring for ledger integrity, and compliance with AML/KYC/KYT, and sanctions screening protocols. Oversight should include regular independent audits of custody infrastructure, transparent governance and escalation processes, and active coordination with regulators to ensure custody practices remain aligned with evolving standards.

Regulations should require custodians to provide transparent, standardized disclosures to customers while maintaining comprehensive internal controls and real-time audit capabilities. Commingling of customer assets for proprietary trading, lending, or other high-risk activities should only be permitted with specific customer consent. Certain forms of pooled lending, staking, or yield generation may require commingling. In such cases, custodians should remain obligated to safeguard customer assets (particularly for retail clients) while permitting greater contractual flexibility for qualified and institutional investors.

Commingling may also be operationally necessary for short periods to settle transactions, facilitate immediate transfer between accounts, or match customer buy/sell orders, similar to how

broker-dealers briefly aggregate funds during the clearing process or trade internalization. Temporary commingling may also be needed to process protocol events like forks, airdrops, or network upgrades. However, regulations should require prompt disaggregation after the event, robust internal controls, and detailed audit trails.

Regulations could also permit custodians to hold digital assets from multiple customers in a single omnibus or pooled blockchain address for technical or security reasons. However, for protection, the Commission should also require that each customer's interests be reflected in segregated, verifiable ledger entries, customers must be able to verify their balances independently, and custodians should be prohibited from rehypothecating or using those assets except as specifically authorized by the customer.

The Commission should not ban or unreasonably restrict the use, development, or maintenance of self-hosted wallets and consumer-controlled private keys. Regulations should also require that banks and traditional financial providers offer nondiscriminatory access for customers transferring funds between traditional accounts and self-hosted wallets, so long as lawful activity is involved and risk assessment protocols are followed. This would prevent "de-risking" or blanket bans that could isolate or disable self-custody users from the broader financial system.

While the RMF does not attempt to prescribe custody rules, it provides a structured method to assess and mitigate the non-financial risks that are central to custody. Phase 1 identifies novel risks on public blockchains such as key management failures, cryptographic vulnerabilities, governance dependencies, and business continuity challenges, all important considerations for ensuring "individuals and organizations can safely, legally, and practicably custody client crypto assets themselves or with a third party."

The RMF suggests the focus should be on demonstrable resilience testing, independent audits of custody technology, contingency planning, and clear governance escalation procedures. For self-custody by registered entities, minimum standards should include multi-layered key management, continuous monitoring, and independent assurance reviews. The RMF is technology-neutral: it emphasizes that rules should differ only where the risk profile diverges, not solely because of their legal classification or technological architecture.

The RMF also emphasizes that the tokenized securities introduce a complex fusion of traditional financial risks with blockchain-specific operational risks. These include issues around operational stability, connectivity and interoperability, safeguarding customer assets, resilience and security, as well as legal certainty and regulatory compliance. Market structure legislation should direct agencies to supervise tokenized systems using existing risk categories, adapted to the new technical environment.

The RMF treats tokenization as a structural/operational change rather than a change in the fundamental legal categorization of a security, focusing on the non-financial risks introduced by blockchain rails and how to control them within existing Enterprise Risk Management / Non-financial Risks frameworks. It emphasizes that security tokens can streamline issuance-to-settlement and

improve transparency, but that adoption hinges on addressing risks such as interoperability, settlement finality, governance, key management/custody, price transparency, and business-continuity planning on public chains. Practical mitigants the Commission could recognize in guidance include: defining and aligning transaction finality standards at issuance, monitoring chains for reorganizations, aligning custody practices with finality conventions, and improving price discovery and listing transparency across venues and chains. These measures are technology-neutral and map cleanly into existing risk taxonomies rather than requiring entirely new prudential categories.

The RMF points out that various jurisdictions have adopted distinct regulatory frameworks to govern tokenized securities, reflecting their unique legal environments and market needs. Approaches differ in their scope, underlying philosophies, and institutional arrangements, with broadly three different approaches: (1) specific legislation to support digital securities and tokenization (Luxembourg and Switzerland); (2) amendment of security rules to accommodate security tokens (Japan); or (3) mandating parallel processes for securities tokens and the underlying security (USA).

Regulators should apply baseline requirements for transparency, operational integrity, and dispute resolution regardless of whether an asset is recorded via traditional ledgers or blockchain. This might include minimum standards for validator governance, system upgrade procedures, data immutability, and access control - all highlighted in the RMF as critical for ensuring system integrity.

The RMF distinguishes between risks arising from permissionless and permissioned infrastructures operating on a public blockchain. Native crypto assets on public, permissionless chains carry higher risks of theft or loss due to consensus vulnerabilities, open governance, and uncertain finality. Custody of these assets depends almost entirely on private key security and resilience of the underlying chain, which creates elevated exposures.

Tokenized permissioned assets inherit certain mitigants from traditional financial frameworks, such as legal enforceability and issuer accountability, but still face custody challenges including interoperability, reconciliation, and around-the-clock operational readiness. From the RMF perspective, native assets present greater inherent risks, though both asset types share common exposures that must be addressed through robust controls. Custody requirements should therefore be calibrated by the nature of the risk, placing greater emphasis on resilience and monitoring for native assets, and on reconciliation and data integrity for tokenized permissioned asset - rather than treating them uniformly or by classification alone.

The RMF explicitly differentiates risk profiles across blockchain types. Private/permissioned networks can use traditional controls (contractual SLAs, defined accountability, standard third-party risk and BCP), reducing exposure to some public-chain risks, but they re-introduce concentration and scalability trade-offs. Public chains (including public permissioned) require adapted controls for decentralized governance, protocol upgrades/forks, probabilistic finality, validator concentration, and 24/7 operations. Accordingly, risk assessments should be calibrated to the underlying chain's governance/finality model and operational assurances, not the tokenization label.

Per the RMF, atomic/T+0 settlement on a single ledger enables automated DvP, reduces counterparty/default risk, and may materially release collateral tied up in legacy processes. Benefits also include real-time transparency and the elimination of reconciliation steps across fragmented ledgers.

The key non-financial risks are finality (probabilistic finality and possible rollbacks during reorganizations), governance/upgrade coordination, and operational resilience of 24/7 blockchain infrastructure. Interoperability and price-discovery frictions can also impact settlement workflows for security tokens. The RMF's concrete mitigants relevant to Commission's policy include:

- requiring clearly defined finality conventions at issuance (conservative finality thresholds for critical transactions);
- active monitoring and contingency procedures for reorgs;
- and transparency standards for venue listings and pricing to reduce fragmentation.

Encouraging sandbox pilots that apply these controls and mapping them into existing custody/"possession and control" interpretations could advance adoption without sacrificing robustness.

GBBC USA strongly supports the SEC's core objectives of market integrity, robust investor protection, and fair, orderly, and transparent markets. We always emphasize that regulatory frameworks must safeguard innovation, competitiveness, and sustainable growth for firms building in the United States. We respectfully submit Phase 1 of the RMF for your consideration and welcome the opportunity to provide further input or convene our contributors to discuss the framework in detail, including the design of upcoming phases.

Links to resources:
- Risk Mitigation Framework – Phase 1
- RMF fact card
- RMF FAQs

Next Phases of RMF:
- Phase 2 (2025): Expansion into on-chain digital payments, covering tokenized deposits, stablecoins, and other settlement assets (confirmed contributors include Canton Foundation and Chainlink). Phase 2 observers: SWIFT, ISSA (International Securities Services Association), UN Joint Staff Pension Fund (UNJSPF), Asian Development Bank, Wyoming Stable Token Commission
- Phase 3 (2026): Extension to native crypto assets, addressing the unique risks of unbacked and permissionless assets

The framework maps the risks across use cases, lifecycle stages, and blockchain types, offering practical guidance aligned with international standards. SEC should consider adopting RMF in its rules, ensuring robust risk mitigation policies and procedures within the regulated financial institutions.

About GBBC:

Global Blockchain Business Council (GBBC) is the trusted non-profit association for the blockchain, digital assets, and emerging technology community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 284 Ambassadors across 124 jurisdictions and disciplines. GBBC USA is the U.S.-focused entity.

GBBC furthers adoption of blockchain and emerging technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chain, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), GBBC Giving, GBBC USA, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).