



Global Blockchain Business Council (GBBC) - USA: Response to the U.S. Department of the Treasury's Request for Comment on GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale (Docket No. TREAS-DO-2026-0496; RIN 1505-AC95)

General Remarks:

Global Blockchain Business Council - USA (“GBBC”) appreciates the opportunity to comment on the Department of the Treasury’s (“Treasury”) notice of proposed rulemaking implementing section 3 of the Guiding and Establishing National Innovation for U.S. Stablecoins (“GENIUS”) Act (the “Proposal”) [[Treasury Stablecoin Proposed Rule](#), 91 Fed. Reg. 53368 (Aug. 18, 2026)]. GBBC supports Treasury’s efforts to establish clear and administrable rules for the issuance, offer, and sale of payment stablecoins in the United States.

GBBC’s comments are limited to selected questions on which GBBC’s existing work may offer practical insight. GBBC’s membership includes banks, payment stablecoin issuers, digital asset service providers, and technology and infrastructure providers. These comments address areas where GBBC’s work offers a common perspective, and individual members may submit their own comments reflecting their specific views. GBBC’s responses draw on the principles set out in the Proposed Risk Mitigation Framework for Non-Financial Risks of Blockchain Infrastructures (“RMF”), developed by Global Blockchain Business Council and Oliver Wyman through a cross-sector working group comprising financial market infrastructures, global systemically important banks, multilateral development banks, and blockchain protocol teams [[RMF](#) § 1.1, p. 7]. The RMF provides financial institutions with guidelines for identifying and mitigating the non-financial risks that arise from the use of public blockchain infrastructure, and one of its stated objectives is to support dialogue with policymakers and regulators on harmonized policy development and rulemaking [[RMF](#) §§ 1.1–1.2, pp. 7–8].

The RMF was not developed to implement the GENIUS Act and is not intended to serve as a compliance standard under it. GBBC nonetheless considers that the principles it reflects may assist Treasury as it develops guidance on the controls and diligence that support compliance with section 3.



About Global Blockchain Business Council and Global Blockchain Business Council - USA:

Global Blockchain Business Council is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, the association comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

Global Blockchain Business Council furthers adoption of digital technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies through education, public-private sector convenings and development of standards.

Global Blockchain Business Council - USA is the non-partisan U.S. – focused entity based in Washington D.C. and focuses on open access education and pragmatic dialogue to support business growth and innovation and to protect consumers.

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

GBBC initiatives: BITA Standards Council (BITA), Capital Markets Risk Mitigation Framework (RMF), GBBC Digital Media, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), Post Trade Distributed Ledger Group (PTDL) and U.S. Blockchain Coalition (USBC).

GBBC USA

Responses to Questions:

Question 1: Is the extraterritorial effect of section 3 of the Act (12 U.S.C. 5902) (as described in this proposed Part 1523) clear or should Treasury provide additional clarity? For example, should Treasury specify in regulatory text the extent to which Part 1523 has extraterritorial effect as to the issuance of payment stablecoins to persons located outside of the United States?

Response:

GBBC's membership comprises more than 500 institutions across 100+ jurisdictions, many of which issue, distribute, or provide services relating to digital assets across borders. For these participants, clarity on the territorial reach of section 3 is important to designing compliant operations.

GBBC understands that the Proposal treats a payment stablecoin as issued in the United States only if, at the time of issuance, the issuer or the person to whom it is issued is located in the United States, and that Treasury does not read the Act to reach issuances in which neither is located in the United States [[Treasury Stablecoin Proposed Rule](#), § 1523.2(b); 91 Fed. Reg. 53376–77, 53390]. GBBC considers this approach helpful. GBBC understands that this approach distinguishes an issuance from the later circulation of a payment stablecoin on a public blockchain, which may be global. GBBC notes, however, that proposed § 1523.1(b) describes the extraterritorial effect of Part 1523 in terms of offers and sales, while the treatment of issuances to persons located outside the United States appears in proposed § 1523.2(b) [[Treasury Stablecoin Proposed Rule](#), §§ 1523.1(b), 1523.2(b); 91 Fed. Reg. 53389–90]. GBBC would welcome conforming the two provisions, or adding a cross-reference, so that this treatment is clear on the face of the rule, particularly given the criminal penalties associated with violations of section 3(a).

The RMF notes that regulatory ambiguity across jurisdictions and the borderless nature of public blockchains can complicate determining applicable law and jurisdictional authority, and it identifies this uncertainty as a source of legal risk for institutions [[RMF](#) § 6.1, p. 42]. GBBC considers clear jurisdictional boundaries in the final rule to be an important means of reducing that uncertainty.

GBBC USA

GBBC would also welcome additional interpretations, similar to proposed Interpretation 1 in Appendix A, illustrating common cross-border fact patterns, such as arrangements between issuers and their affiliates and issuance outside the United States followed by secondary distribution [[Treasury Stablecoin Proposed Rule](#), App. A, Interpretation 1; 91 Fed. Reg. 53391].

GBBC USA

Question 2: Are there any scenarios in which issuing or making available a payment stablecoin would not reasonably be considered an offer or sale? If so, would such activity nonetheless fall within the extraterritorial scope of the Act and this Part? Are there any scenarios in which other conduct or transactions involving a payment stablecoin contemplated by Part 1523 would not reasonably be considered within the extraterritorial scope of the Act?

Response:

GBBC understands that issuance, offer, sale, and making available are overlapping but distinct concepts and would welcome clarification of their boundaries. An airdrop without consideration may constitute issuance without a sale, although the Act's broad definition of "offer" means that the absence of consideration would not alone exclude it from that definition [[Treasury Stablecoin Proposed Rule](#), Question 59 and App. A, Interpretation 2; 91 Fed. Reg. 53383, 53391] [[GENIUS Act](#) § 2(21)]. Consistent with its responses to Questions 19–21, GBBC would also welcome examples addressing technical transfers between networks that preserve the same holder's existing rights without making a payment stablecoin available for purchase, sale, or exchange. Other examples that may be helpful include a transfer to an issuer-controlled treasury or reserve wallet, an internal transfer among wallets controlled by the same person, and collateral or operational movements that do not convey rights to holders.

GBBC understands that the absence of an offer or sale may not, by itself, determine whether an activity falls outside Part 1523. GBBC would welcome clarification of how section 3(e) and proposed § 1523.1(b) interact with the separate issuance provisions, including where an issuance involves a person located in the United States, but no offer or sale occurs. Consistent with its response to Question 1, GBBC understands that Treasury does not intend to capture issuances where neither the issuer nor the recipient is located in the United States [[Treasury Stablecoin Proposed Rule](#), 91 Fed. Reg. 53377]. GBBC would welcome clarification that the use of a globally accessible public blockchain does not, by itself, establish a U.S. territorial nexus. GBBC would also welcome guidance on the types of information Treasury would consider relevant in assessing whether a foreign issuer has the technological capability to comply with lawful orders, as contemplated by section 3(b)(2) of the Act.

GBBC USA

Question 19: Under what circumstances, if any, should the transfer or movement of a payment stablecoin from one blockchain network to another, including through a bridge or similar cross-chain mechanism, be treated as an issuance? Should the treatment depend on the technical structure of the bridging arrangement, including whether the arrangement uses a lock-and-mint, burn-and-mint, liquidity-pool, issuer-operated bridge, third-party bridge, or other mechanism?

Response:

GBBC understands that cross-chain transfers can take different technical forms and would welcome guidance on how the rights and obligations created by an arrangement, considered alongside its technical operation, bear on whether a new issuance has occurred.

The RMF identifies inter-chain connection disruptions and interoperability mechanism failures as key technology risks that may disrupt transfers, create inconsistent asset representations, and increase reconciliation and remediation efforts. It recommends clear governance for supported routes and representations, continuous monitoring, and established procedures to suspend and resume cross-domain activity [[RMF](#) § 5.1, pp. 22–23]. The RMF defines a bridge as a mechanism that typically creates a synthetic asset representation on another blockchain while the original asset remains locked [[RMF](#) Glossary, p. 91]. GBBC finds these insights important in determining whether a cross-chain transaction alters only an asset's technical representation or also creates or transfers a legally distinct claim.

GBBC understands that, depending on how a cross-chain arrangement is structured, questions may arise as to whether a representation of a payment stablecoin on another network continues to satisfy the statutory definition of a payment stablecoin. GBBC would welcome Treasury's views on this question, which GBBC also raises in its response to Question 21.

GBBC would encourage Treasury to consider providing examples addressing transfers of existing tokens through liquidity pools, issuer-operated burn-and-mint migrations, and lock-and-mint arrangements that create a separate representation, including arrangements in which a provider takes custody of assets and those in which a holder uses non-custodial software without the provider taking custody or exercising control. Relevant considerations could include whether the original token remains transferable, whether the holder's claim against the issuer continues unchanged, whether another person assumes a redemption obligation, whether a bridge provider takes custody of the underlying assets or exercises control over the transfer, and whether additional independently exercisable claims arise. GBBC would also welcome

GBBC USA

clarity on what weight, if any, Treasury would give to whether the aggregate amount of payment stablecoins outstanding changes.

GBBC USA

Question 20: Under what circumstances, if any, should a bridge provider, bridge operator, custodian, or other intermediary involved in cross-chain transfers be treated as an issuer of a payment stablecoin? What factors should be relevant to that determination, including control over minting or burning, control over reserve assets, redemption obligations, contractual rights, or the ability to create or retire tokenized claims?

Response:

GBBC understands that the proposed definition of “issuer” turns on the obligation to convert, redeem, or repurchase a payment stablecoin and on representations regarding stable value, and that Treasury has indicated that persons performing technical functions to effectuate minting would not, on that basis alone, be considered issuers [[Treasury Stablecoin Proposed Rule](#), 91 Fed. Reg. 53374]. GBBC would welcome further guidance on how control over a minting key, bridge contract, or custody arrangement would be considered alongside a person’s obligations to holders, representations about stable value, and authority to create or retire claims.

The RMF distinguishes administrative privileges, third-party dependencies and legal accountability. It recommends mapping the parties that can alter system or bridge behavior and documenting responsibilities where counterparties are identifiable [[RMF](#) § 5.2, pp. 30–31; § 5.5, pp. 39–41; § 6.1, pp. 42–43]. The RMF also notes that, where operations are sufficiently centralized and identifiable, institutions may apply traditional third-party controls such as service-level agreements, escalation timelines, and audit rights [[RMF](#) § 4.3, p. 15].

GBBC considers these distinctions, including whether a provider takes custody of assets or exercises discretion over a transaction, relevant to assessing whether an intermediary acts within a defined service mandate or undertakes an independent issuing function.

Illustrative guidance could address the treatment of a provider that executes minting instructions on an issuer’s behalf, a custodian that safeguards assets without assuming a redemption obligation, and an operator that creates a separate tokenized claim and makes its own commitments to holders. GBBC would also welcome clarity on the weight Treasury would give to contractual descriptions relative to actual conduct and control.

GBBC also understands that some cross-chain arrangements rely on non-custodial software that a holder operates independently, without the software provider taking custody of the holder’s assets or exercising discretion or control over a transaction. GBBC would welcome clarification as to whether, and under what conditions, the provision of such software would, on that basis

GBBC USA

alone, result in the provider being treated as an issuer, consistent with Treasury's statement regarding persons performing technical functions [Treasury Stablecoin Proposed Rule, 91 Fed. Reg. 53374].

It would also be helpful to distinguish issuer status from potential participation in an unlawful issuance. GBBC understands that, as Treasury notes, a person that is not an issuer may nonetheless be subject to penalties if it knowingly participates in an unlawful issuance [[Treasury Stablecoin Proposed Rule](#), 91 Fed. Reg. 53374].

GBBC USA

Question 21: Under what circumstances should the creation, minting, distribution, or transfer of a wrapped version of a payment stablecoin, a bridged representation of a payment stablecoin, a deposit receipt, or another tokenized claim referencing a payment stablecoin be treated as a new issuance? Should the analysis depend on the economic or legal rights embedded in the wrapped token, receipt token, or other instrument, including rights to use, transfer, redeem, convert, or obtain the underlying payment stablecoin or related reserve value?

Response:

As an initial matter, GBBC understands that deposits, including deposits recorded using distributed ledger technology, are excluded from the definition of payment stablecoin under the Act, as the Proposal recognizes [[Treasury Stablecoin Proposed Rule](#), 91 Fed. Reg. 53368 n.3] [[GENIUS Act](#) § 2(22)(B)(ii)]. GBBC's response to this question is accordingly limited to wrapped and bridged representations of payment stablecoins.

GBBC would welcome guidance on how the rights and obligations associated with a wrapped or bridged representation bear on whether its creation or transfer constitutes a new issuance, including whether the representation itself satisfies the statutory definition of a payment stablecoin.

The RMF identifies the potential for inconsistent representations across networks and divergence between legal obligations and technical outcomes [[RMF](#) § 5.1, pp. 22–23; § 6.1, pp. 42–43]. It recommends legal review of cross-layer dependencies, clear contractual documentation and procedures for addressing failures [[RMF](#) § 6.1, p. 43]. GBBC considers these principles relevant to understanding which rights a holder can enforce, against whom, and under what conditions.

Treasury may wish to distinguish a representation that preserves the holder's existing claim against the original issuer from an instrument that establishes a separate obligation of another party. Examples could also help explain the difference between a right to receive an underlying digital asset and a right to receive a fixed amount of monetary value, consistent with the statutory definition.

Relevant operational evidence could include how the underlying assets are held, whether they remain transferable, how representations are reconciled, what happens if the bridge or custodian fails, and whether a wrapped representation is created by a custodian or through

GBBC USA

non-custodial software operated by the holder. Further consideration is whether multiple independently exercisable claims can arise.

GBBC USA

Question 28: Does Treasury’s proposed definition of “located in United States” present substantial operational challenges for issuers or risk of evasion by persons to whom tokens are issued? What considerations and capabilities should Treasury take into account to address such challenges and risks?

Response:

GBBC would welcome additional guidance on the evidence issuers may reasonably use to apply the proposed location definition. Customer identity, residence and physical presence are distinct facts, while the proposed treatment of legal entities requires separate information about organization or incorporation and principal place of business.

The RMF recognizes that public blockchain transparency can support monitoring, but pseudonymity complicates identity verification and transaction attribution. Its approach combines off-chain identification with transaction monitoring and other controls [[RMF](#) § 5.3, pp. 31–33]. GBBC therefore considers blockchain addresses and transaction histories to be supporting information rather than conclusive evidence of a person’s physical location.

Further guidance could help issuers assess temporary presence, changes in customer circumstances, and inconsistent information across identification records, customer representations, and device- or network-location indicators. It would also be helpful to explain how these checks apply where issuance occurs through an intermediary.

GBBC would welcome an approach that assesses the reasonableness of the controls and the response to contrary information, rather than assuming that any individual data source provides certainty. Consistent with the RMF’s data-management principles, GBBC considers it appropriate to retain relevant evidence securely off-chain and to avoid unnecessary collection or public disclosure of sensitive customer information [[RMF](#) § 6.3, pp. 46–47].

Question 38: What policies, procedures, or controls should support a reasonable belief that the acquiring person is outside the United States? Should Treasury identify specific controls, such as customer identification and due diligence, account-opening information, geographic access restrictions, device- or network-location checks, contractual representations, transaction monitoring, or other controls? Would this diligence take the form of self-attestations, IP address checking, identification document checking, or something else? If the issuer only directly distributed to a digital asset service provider or other intermediary to make the market or otherwise facilitate the transfer of newly-issued payment stablecoins to the ultimate purchasers, should the issuer's obligations be limited to checking whether the intermediary is located in the United States? Or should the issuer be required or expected to work with the intermediary to confirm whether the ultimate purchasers of newly-issued payment stablecoins are located in the United States? Does a reasonableness standard provide sufficient guidance? Should the policies, procedures, and controls be reviewed and updated on a particular cadence?

Response:

GBBC considers that the reasonableness standard in the Proposal would be well supported by illustrative controls and clear expectations for documentation and escalation. Depending on the distribution model, relevant measures could include verified customer information, contractual representations, geographic access controls, device- or network-location indicators and monitoring for inconsistent information. In GBBC's view, no single measure would be universally sufficient.

This approach draws on the RMF's combination of customer identification, transaction monitoring, vetted counterparties, and ongoing third-party diligence. The RMF also recognizes that controls must address additional entry points and dependencies created by bridges and layered networks [[RMF](#) § 5.3, pp. 31–33; § 5.5, pp. 39–40]. The RMF further contemplates calibrating due diligence, resilience requirements, and monitoring the criticality of the relevant networks and supporting services [[RMF](#) § 4.3, p. 15].

Where an issuer distributes through an intermediary, GBBC would welcome clarity on whether, and under what conditions, the issuer may rely on that intermediary's customer-location checks. GBBC considers the RMF's third-party diligence principles, including upfront assessment of a provider, clear service expectations, and ongoing monitoring of the provider's performance and compliance, relevant to that question [[RMF](#) § 5.5, p. 40]. At the same time, further clarity

GBBC USA

would be helpful on the limits of any obligation to identify subsequent holders outside the issuer's distribution arrangements.

GBBC considers periodic policy reviews according to risk, together with reviews following material changes to distribution channels, relevant technology or identified evasion patterns, to be appropriate. Material inconsistencies or changed circumstances would also warrant refreshing customer-specific information. These controls would operate alongside the other conditions in proposed § 1523.2(c), including its advertising and solicitation restrictions [[Treasury Stablecoin Proposed Rule](#), § 1523.2(c); 91 Fed. Reg. 53390].

GBBC USA

Question 43: Should Treasury set requirements, guidance, or safe harbors relating to how a person should determine if it is participating in an unlawful issuance in accordance with proposed § 1523.2(d)? If so, would they be similar to or different from the requirements, guidance, or safe harbors contemplated in the prior question relating to proposed § 1523.2(c)? Should the requirements differ based on whether the participant in the issuance is the issuer itself, a person providing its branding in a white label arrangement, a market maker, a service provider, or something else? Should one participant be permitted to rely on the representations of another participant that the issuance is lawful? Are such requirements, guidance, or safe harbors appropriate and necessary for § 1523.2 or should § 1523.2 focus instead on the factual contours of participating in an issuance to a person located in the United States, and reserve questions of knowledge or due diligence to the determination of a “knowing” violation under section 3(f)?

Response:

GBBC would encourage Treasury to consider guidance distinguishing the activities that constitute participation in an issuance from the knowledge required for liability under section 3(f) of the Act. Due-diligence guidance could help participants assess their involvement without treating a failure to follow a particular procedure as automatically establishing a knowing violation.

The RMF recommends clear roles, responsibilities and escalation paths, together with diligence proportionate to third-party dependencies and documented legal obligations [[RMF](#) § 4.1, p. 13; § 4.3, p. 15; § 5.5, pp. 39–41; § 6.1, pp. 42–43]. GBBC considers these principles relevant to whether expectations should differ for an issuer, a branding provider, a market maker and a technical service provider, reflecting their actual activities and access to relevant information.

Further guidance could help participants understand when they may reasonably rely on another party’s representations, supported by checks appropriate to their role. Relevant measures could include verification of issuer status, documentation of the distribution arrangement, review of information inconsistent with the representation, and procedures for escalation when circumstances change. Such reliance would not, in GBBC’s view, justify disregarding known contradictory facts.

Examples could also help distinguish ordinary technical services from coordination of key steps in an unlawful issuance. GBBC appreciates Treasury’s use of illustrative interpretations in Appendix A of the Proposal, such as proposed Interpretation 3, and would welcome additional

GBBC USA

examples of this kind [[Treasury Stablecoin Proposed Rule](#), App. A, Interpretation 3; 91 Fed. Reg. 53391]. Clear interpretive guidance could address these issues initially, with any additional safe harbor considered separately in light of Treasury's statutory authority.

Question 52: What due diligence should be required of a digital asset service provider in order for the digital asset service provider to be entitled to rely on the representation of a foreign payment stablecoin issuer that the foreign payment stablecoin issuer has the technological capability to comply, and will comply, with the terms of any lawful order and any reciprocal arrangement pursuant to section 18 of the Act (12 U.S.C. 5916)? Should the rule be more prescriptive about the form of the representation, such as requiring it to be in writing, contain certain language, or be updated with some frequency? Is the requirement to conduct reasonable due diligence clear and appropriate? Should the proposed rule be more prescriptive about the specific steps a digital asset service provider must take? For example, should the rule address certain public representations or advertisements made by foreign payment stablecoin issuers, such as that their payment stablecoins are resistant to freezing? Should the rule require digital asset service providers to retain records of the representation and due diligence, and if so, which records and for how long? For example, should a digital asset service provider be required to audit or examine smart contracts relating to a payment stablecoin? If so, should a digital asset service provider be required to verify the existence and/or efficacy of smart contract functions designed to comply with lawful orders, such as “seize,” “freeze,” and “burn” functions? Would such requirement effectively prevent digital asset service providers from offering, selling or otherwise making available payment stablecoins whose code is not fully open source?

Response:

GBBC agrees with Treasury that permitting a digital asset service provider to rely on a foreign payment stablecoin issuer’s representation, supported by reasonable due diligence, is a practical approach consistent with the purposes of the Act. GBBC also understands that Treasury expects such diligence, at a minimum, to include confirming that no prohibition on secondary trading under section 8 of the Act is in effect with respect to the foreign issuer [[Treasury Stablecoin Proposed Rule](#), 91 Fed. Reg. 53382].

GBBC sees value in guidance identifying the evidence that can support reasonable diligence on a foreign issuer’s technological capability and commitment to comply. GBBC understands that a written representation could be supported by information such as the relevant token contracts, administrative permissions, governance arrangements and procedures for implementing lawful orders. GBBC considers that the depth of this diligence would appropriately be proportionate to the risk presented, consistent with the RMF’s approach of calibrating due diligence and monitoring to criticality [[RMF](#) § 4.3, p. 15].

GBBC USA

The RMF recommends independent contract assurance, testing, clear upgrade and emergency-action authority, privilege controls, and ongoing monitoring. It also addresses the additional dependencies introduced by bridges and Layer 2 systems [[RMF](#) § 5.2, pp. 27–31; § 5.5, pp. 39–41]. In addition, the RMF identifies asset-freezing mechanisms among the process adaptations institutions may need when using public blockchains [[RMF](#) § 4.3, p. 15]. GBBC considers these principles relevant to assessing whether a control operates effectively across the networks and representations offered by the service provider, rather than relying solely on the existence of a function named “freeze,” “seize” or “burn.”

Treasury may wish to consider allowing reliance on appropriately scoped independent assessments, supported where necessary by controlled testing and evidence that the assessed code corresponds to the deployed contracts. Relevant diligence considerations would include who can activate the controls, required approvals, relevant dependencies and known limitations. Such an assessment could help establish the ability to implement the applicable lawful order.

Periodic review of representations and supporting assessments according to risk, together with review following material changes to code, permissions, supported networks or compliance arrangements, could help maintain the reliability of the evidence. GBBC would welcome guidance on how a service provider should consider public claims that appear inconsistent with an issuer’s representation.

Records that could be relevant include representations, assessment scope and findings, relevant testing evidence, material-change records and documented decisions, consistent with the RMF’s recommendation that institutions retain logs to support audits and disputes [[RMF](#) App. A.6, p. 86]. Alignment with applicable recordkeeping requirements could help inform the retention approach. Technical assurance would inform the assessment of capability, while the issuer’s legal commitments, governance and compliance record inform the separate assessment of whether it will comply.

GBBC also notes that the statutory standard addresses compliance with both lawful orders and reciprocal arrangements under section 18 [[Treasury Stablecoin Proposed Rule](#), § 1523.3(b)–(c); 91 Fed. Reg. 53390]. Diligence on a foreign issuer’s ability to comply with reciprocal arrangements may rest more on review of the applicable legal and supervisory arrangements than on technical assessment, and GBBC would welcome guidance on Treasury’s expectations in that respect.

GBBC USA

Question 62: What policies, procedures, or controls should support a reasonable belief that the acquiring person is outside the United States? Should Treasury identify specific controls, such as customer identification and due diligence, account-opening information, geographic access restrictions, device- or network-location checks, contractual representations, transaction monitoring, or other controls? Would this diligence take the form of self-attestations, IP address checking, identification document checking, or something else? Should the policies, procedures, and controls be reviewed and updated on a particular cadence?

Response:

GBBC considers a consistent approach to reasonable belief across issuance and offer or sale activities, adapted to the service provider's role and customer relationship, to be appropriate, and refers Treasury to its response to Question 38.

The RMF supports combining customer identification with transaction monitoring, controlled access and escalation procedures. It also recognizes that monitoring must account for additional entry points and cross-layer activity [[RMF](#) § 5.3, pp. 31–33]. GBBC considers these principles relevant to evaluating the overall effectiveness of a service provider's controls, while recognizing that blockchain data and individual location indicators have limitations.

Further guidance could also help clarify when existing customer information remains sufficient, what events require additional verification, and how checks would operate at the relevant stage of an offer or sale, including through automated channels. GBBC would encourage consideration of an approach that permits appropriate reuse of reliable information while retaining an expectation of further inquiry where material inconsistencies arise. It may also be helpful to explain how customer-location controls interact with the separate restriction on advertising or solicitation directed to persons in the United States.

Consistent with the RMF's data-management principles, GBBC considers it appropriate to minimize and protect sensitive identification and location information and retain it off-chain where appropriate, without assuming that continuous collection of precise physical-location data is necessary [[RMF](#) § 6.3, pp. 46–47].

Conclusion:

GBBC appreciates Treasury's consideration of these comments and would welcome the opportunity to serve as a resource, drawing on the work of the RMF working group and GBBC's broader membership.