Harneys Fiduciary Limited,
4th Floor, Harbour Place,
P.O. Box 10240,
Grand Cayman (KY1-1002)

midnight.foundation

Comment of the Midnight Foundation

GENIUS Act Regulations on Payment Stablecoin Issuance, Offer, and Sale

Docket: TREAS-DO-2026-0496 | **RIN:** 1505-AC95 | **FR Doc:** 2026-16796
Submitted via: regulations.gov
Comment Deadline: October 19, 2026
Date: October 19, 2026
Submitted by: Midnight Foundation | midnight.foundation
Technical Contact: Dr. Saj Khoshroo, Chief Legal Officer | legal@midnight.foundation

---

I. Introduction and Standing

The Midnight Foundation submits this comment as a blockchain infrastructure provider whose selective disclosure architecture directly enables compliant foreign payment stablecoin issuers to operate — and whose architecture is therefore directly implicated by the standards Treasury is now setting. The technical principles underlying these clarifications have implications beyond the foreign payment stablecoin issuer pathway; architecture-neutral standards in Part 1523 will benefit the broader payment stablecoin ecosystem as domestic licensing frameworks develop.

Midnight is a Layer 1 blockchain protocol built on zero-knowledge (ZK) cryptography and selective disclosure principles. The Midnight Network allows token issuers to protect sensitive transaction data from public exposure while preserving the ability to disclose complete, cryptographically authenticated transaction records to authorized parties — including law enforcement and financial regulators — pursuant to lawful process. This architecture is purpose-built for institutional use cases that require both regulatory compliance and data minimization.

The Midnight Foundation is not a payment stablecoin issuer. The NIGHT token is a utility token; its value is not pegged to a fixed amount of monetary value, the Foundation holds no redemption obligation with respect to NIGHT, and NIGHT transactions are publicly visible on the blockchain. The Foundation does not submit this comment as a permitted payment stablecoin issuer or as a party subject to the issuance framework under Section 3.

The Foundation's standing derives from two sources. First, as an infrastructure provider whose architecture is directly implicated by the regulatory standards Treasury is now drafting —

particularly the “technological capability to comply with lawful orders” standard and the due diligence framework for digital asset service providers at proposed §1523.3(c) — the Foundation has direct technical expertise material to the questions Treasury is resolving. Second, the Act’s definition of “payment stablecoin” excludes a deposit as defined in 12 U.S.C. §1813, including a deposit recorded using distributed ledger technology. 12 U.S.C. §5901(22)(B). How that exclusion applies to deposits taken by non-US banks is a boundary question, and institutions in this position therefore have a direct interest in where Treasury draws the line between payment stablecoins and tokenized deposits (cf. Q5) and, to the extent a product is treated as a payment stablecoin, in the conditions Treasury sets for foreign payment stablecoin issuers under proposed §1523.3. This is a real world concern for Midnight which is working to provide the blockchain infrastructure to such non-US banks.

The Foundation previously submitted a comment in response to the FinCEN and OFAC notice of proposed rulemaking on AML/CFT program requirements and sanctions compliance obligations for payment stablecoin issuers (Docket No. FINCEN-2026-0100, June 5, 2026, available at https://www.regulations.gov/comment/FINCEN-2026-0100-0022) (the “FinCEN/OFAC Comment”). That submission established the technical and compliance foundations of Midnight’s selective disclosure architecture in detail. The Foundation incorporates that comment by reference here and does not reproduce its full technical analysis. This submission addresses the distinct questions presented by Section 3’s market access framework.

The Foundation also notes a related regulatory development: on September 30, 2026, Treasury issued an interim final rule establishing the Stablecoin Certification Review Committee’s procedural framework for reviewing state payment stablecoin regulator certifications under GENIUS Act Section 4(c) (12 CFR Part 1522, Docket TREAS-DO-2026-0562). That rule defines state-level regulatory regimes by cross-reference to Treasury’s proposed Part 1521 “substantial similarity” principles, which will in turn be benchmarked against the federal standards being established by this NPRM. Technology-neutral definitions secured in Part 1523 will therefore propagate into the “substantial similarity” baseline against which state regimes will be certified, amplifying the systemic stakes of the clarifications the Foundation urges below.

The Foundation’s core framing applies throughout: **regulatory visibility is not the same as public transparency.** Every compliance obligation Treasury is encoding in this rulemaking — lawful order compliance, due diligence verification, acquirer location assurance — requires that *authorized parties* can access the relevant data. None of them requires that *the general public* can. Selective disclosure gives authorized parties richer and more authoritative access than a public chain provides, while protecting users and institutions from the many harms that permanent public exposure creates. By minimizing the data that is publicly exposed, selective disclosure architectures also reduce the attack surface available to bad actors — what cannot be seen cannot be as easily exploited.

The Foundation submits five targeted clarifications. Each addresses a specific drafting question in the NPRM that, without clarification, risks inadvertently excluding compliant selective disclosure architectures from the US payment stablecoin market — and in doing so, deterring precisely the institutional digital asset innovation that Executive Order 14178, “Strengthening American Leadership in Digital Financial Technology,” directs the federal government to advance. Architecture-neutral standards in Part 1523 are achievable with modest drafting adjustments; without them, the most compliance-capable selective disclosure architectures in

the digital asset ecosystem risk being impeded.

II. Clarification 1 — Architecture Neutrality for "Technological Capability to Comply with Lawful Orders": Proposed §1523.3(c) and Q52

The Question

Q52 asks what due diligence a digital asset service provider must conduct to rely on a foreign payment stablecoin issuer's representation that it has the "technological capability to comply with lawful orders," including orders to seize, freeze, and prevent the transfer of payment stablecoins (12 U.S.C. §5901(16); §5903(a)(6)(B)).

The Concern

If Treasury's guidance implies that "technological capability" must be demonstrated through public ledger verifiability — that is, that a digital asset service provider satisfies its due diligence obligation by querying a public block explorer to confirm issuer compliance — then selective disclosure architectures are effectively precluded from the foreign payment stablecoin issuer pathway, regardless of their actual compliance capability. Nothing in the GENIUS Act requires this outcome, and it would exclude architectures that provide compliance-equivalent or superior performance.

The Argument

On a transparent chain, law enforcement can independently verify compliance by querying a public block explorer. On a selective disclosure chain, verification requires the issuer to provide viewing key data to authorized parties, who can then cryptographically verify the record's authenticity. This introduces an additional step in the enforcement workflow — but it is a step that produces superior evidentiary output, and one that mirrors established practice in traditional finance, where account records and transaction histories are never publicly visible yet are routinely and reliably disclosed to regulators and law enforcement through legal process.

A cryptographically signed, tamper-evident transaction record with a verifiable chain of custody is stronger evidence than a public block explorer query, which can be manipulated through screenshot editing, is unauthenticated, and carries no chain-of-custody guarantee. The FinCEN/OFAC Comment addresses this equivalency in detail (see FinCEN/OFAC Comment, Section IV.E); the Foundation does not reproduce that analysis here.

A selective disclosure foreign payment stablecoin issuer operating on the Midnight network has the technological capability to comply with lawful orders through three distinct mechanisms:

1. Viewing key access. The issuer maintains cryptographic viewing keys that provide full transactional visibility to authorized parties pursuant to lawful process — including law enforcement and regulators. This access is governed by the issuer's operational protocols and

produces cryptographically authenticated records.

2. Smart-contract freeze and burn. Administrative control over the payment stablecoin contract is independent of the privacy architecture. The same freeze, burn, and transfer-prevention mechanisms available on transparent chains are implementable on selective disclosure blockchains.

3. Pre-settlement sanctions screening. The token contract requires every transfer to include a ZK proof that neither party appears in an issuer-maintained sanctions set. Non-compliant transfers are rejected before settlement — a stronger control than post-settlement detection on a public chain.

Proposed Clarification

The Foundation requests that proposed §1523.3(c) confirm that a digital asset service provider may satisfy its "reasonable due diligence" obligation with respect to a foreign payment stablecoin issuer operating on a selective disclosure architecture by verifying, in addition to any other diligence Treasury specifies, that the foreign payment stablecoin issuer: (a) maintains cryptographic viewing keys providing full transactional visibility to authorized parties pursuant to lawful process including law enforcement; (b) has implemented smart-contract-level freeze, burn, and transfer-prevention capabilities; and (c) has the operational governance to respond to lawful orders using those capabilities. Verification via a publicly visible ledger should not be a prerequisite for reasonable due diligence.

III. Clarification 2 — Bridge and Cross-Chain Treatment: Q19–21

The Question

Q19–21 ask when a cross-chain bridge transfer of a payment stablecoin constitutes a new issuance, and when a bridge operator should be treated as the issuer of a payment stablecoin. The proposed factors include control over minting or burning, control over reserve assets, redemption obligations, and contractual rights.

The Concern

If technical control over bridge mechanics — including technical responsibility for lock/mint or burn/mint operations — is treated as sufficient to classify a bridge operator as an issuer, every cross-chain bridge providing services to payment stablecoin infrastructure would become subject to GENIUS Act licensing requirements. This would effectively shut down the cross-chain payment stablecoin ecosystem without a statutory basis for doing so.

The Argument

A third-party bridge operator that facilitates cross-chain movement of an existing issuer's payment stablecoin should not be classified as an issuer of that payment stablecoin unless the operator independently satisfies both elements of the statutory "payment stablecoin" definition:

(1) an obligation to convert, redeem, or repurchase the payment stablecoin for a fixed amount of monetary value; and (2) a representation — or the reasonable expectation — that the operator will maintain stable value. This is the same two-part test Treasury proposes for the definition of "issuer" in §1523.1(c), which the Foundation supports. The Foundation requests, however, that Treasury confirm that the test governs bridge operators regardless of how their minting or burning mechanics are structured (Q20).

Technical control over bridge mechanics does not create a redemption obligation or a stable-value representation. A bridge operator performs a token transfer service; the underlying payment stablecoin's value and redemption obligation remain with the original issuer throughout.

Treasury should distinguish between: (a) bridge operators that facilitate movement of an existing payment stablecoin across chains without assuming an independent redemption obligation — these operators are not issuers; and (b) parties that independently issue a wrapped instrument with a separate redemption obligation — these parties may be issuers, evaluated on the substance of the economic arrangement.

Selective disclosure blockchains depend on cross-chain bridges for liquidity and interoperability. Classification of bridge operators as issuers would impose licensing burdens on infrastructure providers based on technical mechanics rather than economic substance, undermining the payment stablecoin market Treasury seeks to enable.

Proposed Clarification

The Foundation requests that Treasury confirm in the final rule or accompanying interpretive guidance that a third-party bridge operator or cross-chain infrastructure provider that facilitates the transfer of an existing payment stablecoin between blockchain networks is not treated as an issuer of that payment stablecoin, provided that: (a) the operator holds no independent obligation to convert, redeem, or repurchase the payment stablecoin for a fixed amount of monetary value; and (b) the operator makes no representation, and creates no reasonable expectation, that it will maintain a stable value. The analysis should turn on the economic and legal substance of the bridge arrangement, not the technical mechanics of the bridge protocol. Bridge operators face a related exposure under the participation standard in proposed §1523.2(d), which the Foundation addresses in Clarification 5. The two should be read together.

IV. Clarification 3 — ZK-Based Identity Verification as "Reasonable Belief" Standard for Acquirer Location: Q38 and Q62

The Question

Q38 asks what policies, procedures, and controls should support a foreign payment stablecoin issuer's "reasonable belief" that an acquirer of a payment stablecoin is not located in the United States. Treasury's proposed examples include customer identification and due diligence, account-opening information, geographic access restrictions, device and network location

checks, contractual representations, and transaction monitoring. Q62 asks the same question about a digital asset service provider's "reasonable belief" under proposed §1523.3(e), and the Foundation's request below applies equally there.

The Concern

The proposed examples are drawn from conventional identity verification practices. If Treasury's guidance treats these conventional methods as the exclusive means of satisfying the "reasonable belief" standard, selective disclosure foreign payment stablecoin issuers that deploy more technically rigorous ZK-based identity controls would face uncertainty about whether their compliance approach is accepted, despite the fact that ZK identity proofs are, in several material respects, superior to the conventional alternatives.

ZK-based identity proofs are not speculative: leading international regulatory frameworks have already recognized them as viable compliance tools. The European Union's eIDAS 2 regulation (Regulation (EU) 2024/1183) identifies zero-knowledge proofs as a privacy-preserving technology for the European Digital Identity Wallet (Recital 14) and makes selective disclosure a basic design feature (Recital 59). The European Data Protection Board's Guidelines 02/2025 on the processing of personal data through blockchain technologies (v.2.0 final, July 7, 2026) further identifies ZK proofs as an emerging privacy-enhancing technology that can help reduce risks to data subjects. These developments show that zero-knowledge selective disclosure verification is increasingly recognized internationally as compatible with regulatory objectives. Treasury's guidance on the "reasonable belief" standard has an opportunity to align US regulatory expectations with this emerging international consensus — rather than lag behind it.

The Argument

A selective disclosure foreign payment stablecoin issuer can deploy zero-knowledge identity proofs that cryptographically verify a holder's non-US residency status without transmitting or retaining the underlying personal data. This approach provides compliance assurance that is equivalent to — and in several respects stronger than — the conventional controls Treasury describes:

Control	Traditional Approach	ZK Identity Proof
Tamper-evidence	Document scans are falsifiable; IP addresses are VPN-circumventable	ZK proof is cryptographically bound to immutable on-chain commitments
Data minimization	Retains and transmits personal data (address, passport number, etc.)	Verifies the fact without retaining or transmitting underlying personal data
Independent verifiability	Screenshot or database query	Cryptographically reproducible against on-chain commitments

Control	Traditional Approach	ZK Identity Proof
Evasion resistance	IP spoofing and false documentation are well-documented attack vectors	Proof validity requires correct witness; no equivalent spoofing mechanism

The ZK approach is also consistent with Treasury's data minimization objectives and reduces the attack surface for breaches of sensitive customer data — a concern Treasury has recognized in related guidance.

Proposed Clarification

The Foundation requests that Treasury confirm that the policies, procedures, and controls for establishing "reasonable belief" that an acquirer is not located in the United States expressly accommodate zero-knowledge identity proofs as a technically equivalent, if not superior, alternative to traditional identity document review and device/network location checks. The same confirmation should apply to the reasonable-belief standard for digital asset service providers in proposed §1523.3(e) (Q62). Operating on a selective disclosure architecture should not, by itself, be treated as a failure to implement adequate controls.

V. Clarification 4 — Technology-Neutral Drafting in Appendix A

The Question

Appendix A to the proposed rule sets out four interpretations of Part 1523 (91 FR 53391). Treasury invites comment on whether to adopt additional interpretations and on which aspects of Part 1523 they should address (Q78–80).

The Concern

The four interpretations now proposed do not themselves assume a public ledger. The concern is forward-looking. Elsewhere in the NPRM, Treasury's questions describe a payment stablecoin that "exists on the public blockchain" (Q9) and ask whether service providers should audit smart contracts, a requirement Treasury itself notes could effectively exclude coins whose code is not fully open source (Q52). If interpretations added in response to Q80 are framed around transparent-ledger verification in the same way, selective disclosure architectures would face a structural drafting disadvantage that the statute does not require and that straightforward drafting can avoid.

Proposed Clarification

The Foundation requests that any interpretation Treasury adds to Appendix A that addresses verification of issuer compliance or transaction history use outcome-neutral language (for example, “verified transaction record” rather than “publicly observable transaction”). In response to Q80, the Foundation further requests that Treasury adopt interpretations illustrating that (a) a digital asset service provider’s reasonable due diligence under §1523.3(c) may be supported by cryptographically authenticated records disclosed to authorized parties through viewing keys; and (b) zero-knowledge identity proofs may support a “reasonable belief” under §§1523.2(c)(2) and 1523.3(e)(1).

The same principle is set out in the FinCEN/OFAC Comment (Docket No. FINCEN-2026-0100, June 5, 2026), Clarification 7, which the Foundation incorporates by reference.

VI. Clarification 5 — Safe Harbor for Infrastructure Providers: Proposed §1523.2(d) and Q41–43

The Question

Q43 asks whether Treasury should set requirements, guidance, or safe harbors relating to how a person should determine if it is participating in an unlawful payment stablecoin issuance in accordance with proposed §1523.2(d).

The Concern

Proposed §1523.2(d) identifies activities that constitute “participating” in a payment stablecoin issuance that violates Section 3(a). Without a safe harbor, a blockchain infrastructure provider — such as the Midnight Foundation — whose protocol is used by a non-permitted payment stablecoin issuer to deploy a payment stablecoin could inadvertently be deemed to have participated in an unlawful issuance, solely by virtue of providing the underlying network infrastructure. The risk is practical. The Midnight Network is general-purpose infrastructure for applications that need both privacy and regulatory visibility. Independent third parties may build a range of applications on it, which may include tokenized assets and payment instruments. The Foundation does not control the issuance decisions of those parties.

The Argument

Congress excluded from the Act’s definition of “digital asset service provider” both distributed ledger protocols and persons developing, operating, or validating transactions on a distributed ledger. 12 U.S.C. §5901(7)(B). Although that exclusion does not by its terms govern the penalty provision in Section 3(f), it reflects a clear legislative judgment that protocol-level infrastructure is categorically different from the intermediaries Section 3 regulates. Treasury should interpret “participating” in proposed §1523.2(d) consistently with that judgment. The statute’s exclusions turn on what is being done, not on its corporate form. Section 2(7)(B) excludes from the definition of “digital asset service provider” the development or operation of distributed ledger protocols, and the validation of transactions or operation of a distributed ledger. 12 U.S.C. §5901(7)(B)(ii), (iv). The Midnight Foundation develops the Midnight protocol and supports the Midnight Network. It does not issue payment stablecoins and does not custody stablecoin

reserves.

Proposed §1523.2(d) gives three non-exhaustive examples of participation: incurring an obligation to convert, redeem, or repurchase the payment stablecoin; coordinating with an issuer on key steps in an issuance, such as soliciting customers or minting; and acting as a market maker for newly issued coins, distributing them to purchasers, or otherwise making them available for secondary market trading. See 91 FR 53378. Each describes conduct directed at a particular issuance. A protocol provider that maintains software available to all comers and processes transactions under protocol rules does none of these. Treasury has explained that the second and third examples are meant to capture persons who provide substantial assistance to the issuer at or around the point of issuance, and that the third is not intended to reach secondary market trading without a close temporal nexus to the initial issuance. Treasury has also explained that persons performing technical functions to effectuate minting are not issuers but may face penalties if they knowingly participate. See 91 FR 53374. Because the examples are non-exhaustive (Q41) and the penalty is criminal, the absence of any stated boundary leaves infrastructure providers to guess where a technical function ends and participation begins. Treasury itself invokes Executive Order 14294, "Fighting Overcriminalization in Federal Regulations," for the principle that regulations carrying criminal penalties should explicitly describe the conduct subject to enforcement (see 91 FR 53376–77 n.45). Neutral infrastructure offered on the same terms to every user involves no assistance directed at a particular issuer, and the Foundation asks Treasury to say so.

The risk, however, is that proposed §1523.2(d)'s "participating" standard, absent a safe harbor, creates residual uncertainty for infrastructure providers about whether protocol-level activities, such as processing transactions, validating blocks, or developing smart contract tooling, could be construed as participation in an unlawful issuance. This uncertainty would chill precisely the infrastructure investment that the GENIUS Act and Executive Order 14178 are designed to encourage.

Proposed Clarification

In response to Q41–43, the Foundation requests that Treasury confirm, in the final rule or interpretive guidance, that a person is not deemed to "participate" in an unlawful issuance under §1523.2(d) solely by reason of: (a) developing, maintaining, or operating a distributed ledger protocol or network on which a payment stablecoin is deployed, or validating or processing transactions involving it; (b) publishing protocol-level tooling, smart contract frameworks, software development kits, documentation, or technical support that is generally available to developers on the same terms regardless of application; or (c) developing or operating cross-chain messaging or bridging software that moves an existing payment stablecoin between networks, where the operator has no independent redemption obligation and makes no stable-value representation (see Clarification 2).

This protection should apply where the person (i) does not coordinate with the issuer on soliciting purchasers of, minting, or distributing that issuer's payment stablecoin; (ii) derives no economic benefit tied specifically to that issuance, other than network fees or other compensation generally applicable to all users of the network; and (iii) exercises no control over the issuance, redemption, or reserve management of that payment stablecoin.

Separately, in response to Q43, a person should not be deemed to have knowingly participated

in an unlawful issuance where it reasonably relied on the issuer's written representation, or on publicly available evidence such as an OCC registration or other regulatory authorization, that the issuer is a permitted payment stablecoin issuer or a foreign payment stablecoin issuer meeting the criteria of section 18(a), absent actual knowledge to the contrary.

This clarification is consistent with the GENIUS Act's own treatment of distributed ledger protocols as categorically distinct from digital asset service providers, and with Treasury's stated objective of fostering infrastructure investment in support of the US payment stablecoin ecosystem.

VII. Summary of Proposed Clarifications

The Foundation's five requested clarifications are as follows:

1. Lawful order due diligence (§1523.3(c), Q52). Confirm that a digital asset service provider satisfies its "reasonable due diligence" obligation with respect to a foreign payment stablecoin issuer operating on a selective disclosure chain by verifying, in addition to any other diligence Treasury specifies, the foreign payment stablecoin issuer's viewing key framework, smart-contract freeze/burn capabilities, and governance for responding to lawful orders. Public ledger verifiability is not a prerequisite.

2. Bridge and cross-chain treatment (Q19–21). Confirm that a third-party bridge operator facilitating cross-chain movement of an existing payment stablecoin is not treated as its issuer absent an independent redemption obligation and stable-value representation. The test should turn on economic and legal substance, not technical bridge mechanics.

3. ZK identity verification for acquirer location (Q38, Q62). Confirm that the policies, procedures, and controls supporting a "reasonable belief" that an acquirer is not located in the United States expressly accommodate zero-knowledge identity proofs as a technically equivalent, if not superior, alternative to traditional identity document review and device/network location checks, for both issuers (§1523.2(c)) and digital asset service providers (§1523.3(e)), and that operating on a selective disclosure blockchain does not, by itself, constitute a failure to implement adequate controls.

4. Technology-neutral Appendix A language. Use outcome-neutral verification language in any interpretation added to Appendix A, and adopt interpretations (Q80) showing that authenticated viewing-key records and zero-knowledge identity proofs can satisfy the due diligence and reasonable-belief standards, consistent with the architecture-neutral approach recommended in the FinCEN/OFAC Comment.

5. Safe harbor for infrastructure providers (§1523.2(d), Q41–43). Confirm that a distributed ledger protocol developer, network operator, validator, or cross-chain bridge operator is not deemed to "participate" in an unlawful issuance solely by providing generally available infrastructure, tooling, or support, provided it does not coordinate with the issuer on that issuance, has no issuance-specific economic interest, and has no control over issuance, redemption, or reserves; and confirm that reasonable reliance on an issuer's representation or public regulatory status defeats "knowing" participation absent actual knowledge to the contrary.

VIII. Conclusion

Each clarification the Foundation requests is consistent with — and directly supportive of — Treasury's stated objectives for the GENIUS Act: providing regulatory certainty for payment stablecoin innovation, cementing the US dollar's role in digital finance, and maintaining US leadership in the global digital asset market.

Selective disclosure architectures are not a workaround to compliance obligations. They are a more rigorous implementation of the same compliance outcomes — regulatory visibility without public exposure — that the GENIUS Act demands. The clarifications requested in this comment would confirm that the regulatory framework Treasury is building is genuinely technology-neutral and pro-innovation, and would allow compliant selective disclosure foreign payment stablecoin issuers to participate in the US payment stablecoin market on the same terms as their transparent-chain counterparts.

The Midnight Foundation welcomes the opportunity to provide technical demonstrations of its ZK architecture and selective disclosure compliance capabilities to Treasury staff. Questions regarding the technical content of this submission may be directed to Dr. Saj Khoshroo, Chief Legal Officer, Midnight Foundation (legal@midnight.foundation).

Respectfully submitted,

Dr. Saj Khoshroo, Chief Legal Officer
Midnight Foundation
legal@midnight.foundation

Date: October 19, 2026