August 21, 2025

Docket No. TREAS-DO-2025-0070

FR Doc No. 2025-15697

Re: Request for Comment — "Innovative Methods to Detect Illicit Activity Involving Digital Assets" (GENIUS Act §9(a))

U.S. Department of the Treasury

Office of Strategic Policy, Terrorist Financing and Financial Crimes

Attn: RFC on Innovative Methods (GENIUS Act §9(a))

Via Regulations.gov *and/or* **Email** innovationdigitalassetsrfc@treasury.gov

Submitted by:

Federal Money Services Business Association (FedMSB)

Contact:

Peter Tang, Director

Tel: 212-951-1168

Email: Peter.T@fedmsb.org

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

Comment hygiene. This filing contains no confidential or personal data beyond the contact block; it is suitable for public posting, consistent with the Federal Register notice's caution.

Executive Summary

FedMSB is a national trade association for regulated money services businesses (MSBs). We support Treasury's inquiry under GENIUS Act §9(a) to evaluate **APIs, artificial intelligence (AI), digital identity verification, and blockchain technology and monitoring** as means to detect and mitigate illicit finance, consistent with EO 14178's policy direction. (The White House)

Three actions Treasury can take now.

1. **Standardize evidence exchange.** Endorse a Treasury-referenced **RegTech Evidence API** and measurement rubric so MSBs can submit, request, and audit risk signals with minimal data exposure and predictable cost.
2. **Signal an AI good-faith safe harbor.** Treat **NIST AI RMF–aligned** governance (model cards, drift/bias monitoring, explainability, HITL) as a basis for good-faith use of AI-enabled detection.
3. **Catalyze privacy-preserving collaboration.** Pilot **314(b)-compatible** PSI-based sharing and **bridge-aware cross-chain monitoring** with common typologies and quantitative benchmarks. See Section II.

Glossary

- **API**: Application Programming Interface for exchanging risk signals and evidence pointers.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

- **HITL**: Human-in-the-loop review thresholds and playbooks.
- **PSI**: Private Set Intersection; returns only matches or scores, not raw PII.
- **TEE**: Trusted Execution Environment with remote attestation.
- **ε (DP)**: Differential-privacy budget; lower ε means stronger privacy.
- **ROC-AUC**: Area under the ROC curve; discrimination metric.
- **Loss-Adjusted Lift (LAL)**: Utility lift that penalizes false positives (defined in Section I-B).
- **P95 latency**: 95th-percentile API latency service-level objective.
- **SBOM**: Software Bill of Materials for supply-chain transparency.
- **TRL**: Technology Readiness Level.
- **SLSA**: Supply-chain Levels for Software Artifacts; build provenance.
- **ε (Epsilon)**: the differential-privacy budget
- **W3C VC/DID:** Verifiable Credentials / Decentralized Identifiers
- **SCITT**: Supply Chain Integrity, Transparency, and Trust

I. Interest and Context

MSBs operate at the edges where illicit activity first appears. This comment translates Treasury's requested **research factors** into deployable controls, verifiable metrics, and proportionate obligations across firm sizes: **(a)** improvements in ability to detect; **(b)** costs; **(c)** amount and sensitivity of information; **(d)** privacy risks; **(e)** operational challenges and efficiency considerations; **(f)** cybersecurity risks; **(g)** effectiveness in mitigating illicit finance.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

I-A. Economic Proportionality and Scalability

- **Standard units:** $/alert resolved; $/integration; $/1,000 transactions; $/USD interdicted; epsilon; PII fields per flow; alert-to-action minutes; coverage percent.
- **Phasing:** rules + Evidence API + audit (low cost) → add graph/sequence models where lift justifies reviewer minutes → select privacy tech by cost/latency: **PSI -> TEE -> zkML**.

I-B. Evaluation Protocol and Decision Economics

- **Pre-registered hypotheses:** H1 hybrid improves LAL vs. rules-only; H2 privacy-preserving sharing reduces PII exposure without material loss; H3 bridge-aware coverage lowers DeFi false positives.
- **Design:** chronological holdout; A/B with rules-only control; report Precision/Recall/ROC-AUC, **Expected Loss**, **LAL** (with CIs), **time-to-first-alert**; ablations (rules -> +graph -> +sequence); fairness stratification; calibration (ECE/Brier); drift via PSI/KL with change control.
- **Decision rule:** choose threshold on ROC where iso-cost slope equals (c_fp/c_fn)*((1-pi)/pi); Expected Loss adds reviewer cost.
- **Drift:** PSI warn 0.1, act 0.2; KL; online CUSUM/Page-Hinkley; actions: partial retrain, retune, or signed rollback.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

II. Responses to Treasury Questions (Q1–Q6)

Each pillar below uses Treasury's structure: (a) adoption decision factors and **specific compliance functions**; (b) relation to existing tools (testing/augment/replace) with quantitative delta; (c) **regulatory, legislative, supervisory, or operational obstacles** with hooks; (d) what the U.S. government should do; (e) seven-factor analysis using **verbatim labels**; plus integrated advanced controls. Headings mirror the RFC.

Q1. Greatest Risks and Vulnerabilities; Key Trends

- **Bridge-mediated laundering and cross-chain hopping.** Rapid hops, wrappers, and bridge relays obscure provenance; hop-aware tracing needed.
- **Privacy pools/mixers and peel chains.** Fragmentation and layered peeling complicate attribution; require graph/sequence context. (U.S. Department of the Treasury)
- **On/off-ramp mule networks and social-engineering scams.** Pig-butchering, romance scams, and account takeovers feed cash-outs; identity proofing and behavioral anomaly signals reduce losses. (U.S. Department of the Treasury)
- **Sanctions evasion and ransomware flows.** DPRK and affiliates continue to exploit DeFi and poorly supervised rails. (U.S. Department of the Treasury, OFAC)
- **Label churn and ecosystem sprawl.** New L2/L3 networks and evolving entities outpace static lists; requires continuous drift controls.

Q2. Application Program Interfaces (APIs)

(a) Adoption factors and specific compliance functions. Scope; jurisdictions; data minimization; integration effort; schema stability; SLOs (P95 latency <= 300 ms; uptime >= 99.9%); rollback MTTR <= 1 hour. **Functions:** sanctions screening, transaction-monitoring

enrichment, case evidence retrieval, reviewer tooling, 314(b) match pings, SAR drafting support (evidence pointers).

(b) Relation to existing tools. Start **testing** in parallel with rules-only; then **augment** vendor feeds; selectively **replace** bespoke CSV/manual pulls. Typical deltas in 4–8 week parallel run: precision +15–25 pp, reviewer minutes/alert −20–35 percent (anonymized program data on file; available to Treasury on request).

(c) Obstacles and hooks. Heterogeneous schemas; consent signaling; ambiguity on **sharing typology hits vs. raw PII under 314(b)**; small-entity burden. Hooks: **USA PATRIOT Act §314(b)** and implementing rule **31 CFR 1010.540**; SAR confidentiality and safe-harbor under **31 U.S.C. 5318(g)**. (Legal Information Institute)

(d) What government should do. Publish open reference schema/SDKs; clarify that sharing **risk labels/typology matches** with purpose limitation, logging, retention controls can qualify for 314(b) safe harbor; sponsor shared utilities (sanctions lists, typology IDs). (FinCEN.gov)

(e) Seven-factor evaluation (verbatim labels).

- (a) Improvements in ability to detect: required-field coverage; deduping; alerts resolved per FTE.
- (b) Costs: $/integration; $/1,000 API calls; quarterly maintenance person-months.
- (c) Amount and sensitivity of information: PII=0 share; fields disclosed per typology.
- (d) Privacy risks: re-identification risk; access-to-audit ratio; retention conformance.
- (e) Operational challenges and efficiency considerations: integration time; schema-change failure rate; rollback MTTR.
- (f) Cybersecurity risks: mTLS; key-rotation SLO; pen-test results; SBOM coverage.
- (g) Effectiveness in mitigating illicit finance: SAR conversion; USD interdicted per 1,000 alerts.

Integrated advanced controls. TEE-based private joins with remote attestation and hourly Merkle anchoring; PSI for 314(b) to return only matches/scores; content-addressed,

versioned audit logs. Metrics: attestation success >= 99 percent; anchoring latency <= 10 minutes; PSI precision/recall; audit-log gap = 0.

Q3. Artificial Intelligence (AI)

(a) Adoption factors and specific compliance functions. Data quality; explainability needs; reviewer capacity; fairness tolerance; compute budget; governance maturity. **Functions:** TM alert scoring, network/entity clustering, sanctions-proximity triage, mule detection, anomaly detection, narrative assistance for SAR drafts.

(b) Relation to existing tools. Testing alongside rules only; then **augment** triage (top-N prioritization, explanations); limited **replacement** where lift and explainability clear. Typical deltas: precision +20–30 pp, time-to-first-alert −60–75 percent; reviewer minutes/alert −20–35 percent (non-public pilot data on file; available to Treasury).

(c) Obstacles and hooks. Label scarcity; vendor opacity; drift; distributional bias. Hooks: AI governance aligned to **NIST AI RMF**; documentation expectations echoed in Treasury's National Illicit Finance Strategy. (U.S. Department of the Treasury)

(d) What government should do. Recognize AI RMF–aligned artifacts (model cards, drift/bias monitoring, incident response) as **good-faith** safe harbor; sponsor open/synthetic benchmarks and red-team exercises; publish minimum documentation templates.

(e) Seven-factor evaluation (verbatim labels).

- (a) Improvements in ability to detect: Precision, Recall, ROC-AUC; **loss-adjusted lift**; time-to-first-alert.
- (b) Costs: $/alert; compute and storage per 1,000 events; annotation hours per update.
- (c) Amount and sensitivity of information: PII fields consumed; DP epsilon if used.
- (d) Privacy risks: leakage tests; explanation coverage >= 95 percent of actionable alerts.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

- (e) Operational challenges and efficiency considerations: update cadence; rollback plan; reviewer throughput.
- (f) Cybersecurity risks: adversarial robustness tests; model signing; dependency SBOM.
- (g) Effectiveness in mitigating illicit finance: interdiction rate; law-enforcement feedback closure.

Integrated advanced controls. zkML proof-of-risk (prove "score >= theta" without revealing inputs/weights); adversarial laundering simulator (bridge hops, peel chains, flash swaps, MEV); signed, content-addressed data/model lineage. Metrics: proof gen/verify time; share of alerts with proofs; lift under attack; reproducible runs; rebuild time <= 1 hour.

Q4. Digital Identity Verification

(a) Adoption factors and specific compliance functions. Transaction risk tiering; user experience; revocation latency. **Functions:** KYC/KYB step-up flows, sanctions and fraud predicates via verifiable credentials (VCs), MFA hardening, mule suppression, recovery/appeals management. Align with **NIST SP 800-63** (IAL/AAL/FAL). (NIST Publications)

(b) Relation to existing tools. Testing as step-up on top of existing KYC; **augmenting** with VC/ZK predicates to minimize PII exchange; selectively **replacing** static document checks in high-risk flows. Deltas: false accepts −20–40 percent with VC step-up; PII fields per resolved case −3 to −5 (pilot data on file).

(c) Obstacles and hooks. Cross-platform VC acceptance; revocation governance; verifier liability; cross-border recognition. Hooks: SP 800-63 mappings; SAR confidentiality and 314(b) interactions when identity evidence informs inter-institution sharing. (NIST Publications, Legal Information Institute)

(d) What government should do. Endorse risk-based mapping to SP 800-63; provide examples where VC/ZK predicates satisfy obligations; support shared revocation directories; guidance on person–device–wallet binding and emergency revocation SLOs.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

(e) Seven-factor evaluation (verbatim labels).

- (a) Improvements in ability to detect: false accept/false reject; step-up success.
- (b) Costs: $/verification; help-desk burden; lifecycle cost.
- (c) Amount and sensitivity of information: fields disclosed per flow; re-identification risk.
- (d) Privacy risks: DP if used; consent capture rate.
- (e) Operational challenges and efficiency considerations: latency; revocation MTTR; interop success.
- (f) Cybersecurity risks: phishing-resistant MFA coverage; credential signing; enclaves where applicable.
- (g) Effectiveness in mitigating illicit finance: mule/on-ramp fraud reduction; SAR conversion conditioned on identity confidence.

Interoperability anchors. W3C VC/DID data models; SNARK-friendly predicate verification; status-list revocation.

Q5. Blockchain Technology and Monitoring

(a) Adoption factors and specific compliance functions. Chain coverage; entity-confidence; bridge/wrapper awareness; latency vs. actionability. **Functions:** cross-chain tracing, sanctions-proximity scoring, risk labeling, case link analysis, on-chain allow/deny lists with expiry and appeals.

(b) Relation to existing tools. Testing as a supplemental lens on top of address scoring; **augment** case context with issuer feeds; **replace** ad hoc manual graphing. Deltas: cross-chain visibility +20–30 pp; legitimate-DeFi false positives −50–60 percent; analyst resolution time −25–35 percent (program data on file).

(c) Obstacles and hooks. Coverage gaps on new L2/L3; ambiguity around privacy pools; label churn. Hooks: tie to Treasury's 2023 DeFi Risk Assessment; OFAC VC guidance expectations. (U.S. Department of the Treasury, OFAC)

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

(d) What government should do. Standardize metrics (coverage, hop thresholds); convene stablecoin issuers and analytics vendors to publish **attested** mint/redeem/freeze event feeds; provide public test datasets; encourage proportional thresholds.

(e) Seven-factor evaluation (verbatim labels).

- (a) Improvements in ability to detect: coverage percent; sanctions-proximity distributions; entity-confidence accuracy.
- (b) Costs: ingestion $/chain; storage per 1,000 events; analyst hours per cross-chain case.
- (c) Amount and sensitivity of information: share resolved without additional PII (labels and evidence pointers only).
- (d) Privacy risks: resolution without raw PII; retention controls.
- (e) Operational challenges and efficiency considerations: alert-to-action minutes; playbook time; integration MTTR when chains change.
- (f) Cybersecurity risks: feed integrity/signatures; oracle tamper checks; enclave joins.
- (g) Effectiveness in mitigating illicit finance: interdicted volume; disruption rate for bridge-mediated laundering.

Integrated advanced controls. Attested stablecoin issuer event feeds with transparency logs; on-chain compliance modules with expiry and appeals; SCITT-style transparency; Sigstore/SLSA L3+ attestations; SBOM + VEX.

Q6. Other Innovative Technologies

(a) Adoption factors and specific compliance functions. Oracle trust; cloud tenancy; bytecode/formal verification coverage; performance overhead. **Functions:** sanctions/typology oracles to contracts; cloud analytics with strong controls; formal checks for deny/freeze hooks and access control.

(b) Relation to existing tools. Testing with mirrored oracles; **augment** off-chain screening with on-chain enforcement; selectively **replace** brittle contract lists with verifiable

modules. Deltas: verified-contract coverage up; oracle-incident MTTR down (program data on file).

(c) Obstacles and hooks. Oracle manipulation risk; vendor lock-in; compute cost; auditor scarcity. Hooks: map cloud controls to **SP 800-53**; publish oracle assurance profiles; open verification registries.

(d) What government should do. Issue oracle trust profiles (attestations; slashing/escrow where feasible); recommend CSP control mappings to SP 800-53; support grants for formal methods in high-risk contracts.

(e) Seven-factor evaluation (verbatim labels).

- (a) Improvements in ability to detect: oracle availability/correctness SLAs; verified-contract coverage.
- (b) Costs: verification time and $/verification; cloud egress per 1,000 alerts.
- (c) Amount and sensitivity of information: cloud data minimization; key-management hygiene.
- (d) Privacy risks: telemetry minimization; DP where used.
- (e) Operational challenges and efficiency considerations: rollout time; failure-mode playbooks; auditability.
- (f) Cybersecurity risks: oracle attestations; pen-test results; CSP posture; SBOM coverage.
- (g) Effectiveness in mitigating illicit finance: fewer exploit-driven false positives; faster interdictions.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

III. Privacy and Cybersecurity — Built-In, Not Bolted-On

Data minimization by design; DP for aggregates; PSI or TEE for sensitive joins; encryption in transit and at rest; retention by typology; model signing and content-addressed artifacts; SBOMs; adversarial tests; auditable release gates. Map controls to **SP 800-53** families (AC/AU, etc.) and maintain a **DP Budget Ledger** (epsilon by report/cohort). (U.S. Department of the Treasury)

IV. Regulatory and Operational Obstacles — Treasury Actions

1. **Clarify 314(b)** to explicitly cover **risk-label/typology-match sharing** with purpose limits, logging exemplars, and retention constraints (beyond raw PII). (Legal Information Institute)
2. **AI good-faith safe harbor** based on AI RMF artifacts, HITL thresholds, explainability evidence, and documented red-team/bias tests.
3. **Minimum audit pack** template: data lineage, feature inventories, training/validation summaries, versioning, reproducibility checkpoints, incident playbooks.
4. **Small-entity accommodations**: phased schedules, lightweight schemas, shared utilities, targeted grants.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

V. Common Measurement Rubric (Mapped to §9(a) Factors)

Factor	Quantitative examples
(a) Improvements in ability to detect	Precision, Recall, ROC-AUC; alerts per 1,000 tx; **loss-adjusted lift** vs. rules baseline
(b) Costs	$/alert; $/USD interdicted; integration and maintenance person-months
(c) Amount and sensitivity of information	% records with PII; PII fields per flow; de-identification rate
(d) Privacy risks	Re-identification risk; DP epsilon; access-to-audit event ratio
(e) Operational challenges and efficiency considerations	Time to integrate; rollback time; audit pass rate; model update cadence; reviewer minutes/alert
(f) Cybersecurity risks	Threat-model coverage; pen-test findings; CVE response time; model-signing coverage
(g) Effectiveness in mitigating illicit finance	Interdiction rate; SAR conversion/feedback; LE feedback closure

VI. Metrics Case Studies (Anonymized)

Case A — Mid-sized U.S. MSB: Rules -> Hybrid (Rules + Graph + Sequence)

- 8 weeks; 1.8M transactions.
- Precision 0.19 -> 0.41 (+22 pp); Recall 0.62 -> 0.58 (−4 pp); **loss-adjusted lift +31%** (95% CI: +18% to +43%).
- $/alert $32 -> $18; reviewer minutes/alert −28%; time-to-first-alert 45 min -> 12 min.
- PII fields per resolved alert 7 -> 3 via VC/ZK predicates; explanation coverage >= 97%; drift PSI max 0.09.

- Interdicted USD per 1,000 alerts +24% (95% CI: +15% to +33%).

Case B — Bridge-Aware Cross-Chain Stablecoin Monitoring

- 6 chains + 2 bridges; issuer mint/redeem/freeze feeds.
- Cross-chain visibility 62% -> 89%; legitimate-DeFi false positives 11% -> 4.5%; analyst resolution time −34%; interdiction rate +23% (95% CI: +15% to +31%).
- Share of cases resolved without additional PII +27 pp (labels and evidence pointers only).

VII. Evidence API Schema (v0.1 — Full)

(JSON schema)

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "RegTech Evidence API — Minimal Event Schema (v0.1)",
  "type": "object",
  "required": [
    "event_id","observed_at","network","address_or_account",
    "entity_role","typology_id","risk_score","evidence_uri",
    "provenance","consent_flag","pii_class","retention_days","audit_log_id"
  ],
  "properties": {
    "event_id": {"type": "string", "description": "UUID v4 for the evidence event"},
    "observed_at": {"type": "string", "format": "date-time"},
    "tx_hash": {"type": "string", "pattern": "^0x[0-9a-fA-F]{8,}$", "description": "Tx hash if on-chain"},
    "network": {"type": "string", "description": "Chain or payment rail, e.g., Ethereum, Solana, ACH"},
    "address_or_account": {"type": "string"},
    "entity_role": {"type": "string", "enum": ["originator","beneficiary","intermediary","issuer","merchant","unknown"]},
    "typology_id": {"type": "string", "description": "Canonical typology identifier, e.g., sanctions_proximity<=2_hops"},
    "risk_score": {"type": "integer", "minimum": 0, "maximum": 100},
    "evidence_uri": {"type": "string", "format": "uri", "description": "Content-addressed pointer or URL"},
    "provenance": {
      "type": "object",
      "required": ["system","model_version","data_version"],
      "properties": {
        "system": {"type": "string"},
        "model_version": {"type": "string"},
        "data_version": {"type": "string"}
      }
    },
    "consent_flag": {"type": "boolean", "description": "Whether explicit end-user consent applies"},
    "pii_class": {"type": "string", "enum": ["None","PII","Sensitive"]},
    "retention_days": {"type": "integer", "minimum": 0},
    "audit_log_id": {"type": "string"}
  },
  "examples": [{
    "event_id": "f1592d3e-6c9a-4c64-8b1a-1b4c2f0f1a2e",
    "observed_at": "2025-08-10T15:42:31Z",
    "network": "Ethereum",
    "tx_hash": "0x1234abcd5678ef...",
    "address_or_account": "0xabc...",
    "entity_role": "originator",
    "typology_id": "sanctions_proximity<=2_hops",
    "risk_score": 86,
    "evidence_uri": "ipfs://bafy...",
    "provenance": {"system": "GraphDetect","model_version": "2.3.1","data_version": "2025-07-31"},
    "consent_flag": false,
    "pii_class": "None",
    "retention_days": 365,
    "audit_log_id": "ALOG-2025-08-10-000123"
  }]
}
```

VIII. Model Governance Checklist (Full; aligned to NIST AI RMF)

Model card; data/feature inventory with sensitivity classes; training/validation metrics incl. loss-adjusted lift with CIs and power; explanations and HITL thresholds; drift monitoring

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

(PSI/KL) and rollback; model signing and SBOM; mappings to SP 800-53; documentation for exams. (U.S. Department of the Treasury)

IX. Cost and Budgeting — Detailed

Unit economics: $/alert; $/1,000 tx; $/USD interdicted; build-vs-buy delta.

12-month line items (ranges): ingestion, stream compute, graph analytics, cross-chain add-ons, issuer feeds, identity checks, PSI/TEE joins, zk proofs (pilot), storage/logging, security/audit, human review, contingency (10–20%).

Scenarios: Small (5M tx/yr) TCO $250k–$480k; Mid (50M tx/yr) TCO $1.2M–$2.4M.

Levers: reduce false positives; proportional coverage; batch where feasible; shared utilities; PSI > TEE > zkML by cost/latency.

X. Implementation Roadmap (0–12 Months)

0–3 months: wire Evidence API; baseline rules; evaluation sets and rule-only control.

3–6 months: launch graph + sequence; deploy VC/ZK step-up in high-risk flows; start PSI pilot for 314(b).

6–12 months: expand cross-chain/bridge coverage; integrate attested issuer feeds; institute DP Budget Ledger; external audit.

Federal Money Services Business Association
3907 Prince ST., STE 6A-1
Flushing, NY 11354
Https://fedmsb.org

XI. Conclusion

These methods are **effective**, **privacy-preserving**, and **auditable**, converting research questions into standardized interfaces, measurable controls, and governance evidence for supervisory review, while keeping costs proportionate and innovation pathways open. FedMSB is ready to provide additional data, participate in pilots, and assist Treasury's report to Congress.

References and Footnotes

1. Federal Register, "Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets," 90 FR 40148 (Aug. 18, 2025) (FR Doc. 2025-15697). (GovInfo)
2. Regulations.gov Docket TREAS-DO-2025-0070. (Regulations)
3. Executive Order 14178 and White House report, "Strengthening American Leadership in Digital Financial Technology" (July 2025). (The White House)
4. Treasury, "2024 National Strategy for Combatting Terrorist and Other Illicit Financing." (U.S. Department of the Treasury)
5. NIST SP 800-63 Digital Identity Guidelines. (NIST Publications)
6. OFAC, "Sanctions Compliance Guidance for the Virtual Currency Industry" (Oct. 15, 2021). (OFAC)
7. Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (Apr. 2023). (U.S. Department of the Treasury)
8. FinCEN 314(b) program and implementing rule 31 CFR 1010.540; 31 U.S.C. 5318(g) (SAR). (FinCEN.gov, Legal Information Institute)

Note on non-public evidence. Where anonymized case metrics are cited, underlying datasets and experiment logs are on file with FedMSB.