4810-AK-P

DEPARTMENT OF THE TREASURY

Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets

AGENCY: Departmental Offices, Department of the Treasury.

ACTION: Request for comment.

SUMMARY: The U.S. Department of the Treasury invites interested members of the public to provide input on the use of innovative or novel methods, techniques, or strategies to detect and mitigate illicit finance risks involving digital assets. This notice fulfills a requirement of the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) and supports the Administration's policy of supporting the responsible growth and use of digital assets, as outlined in the January 23, 2025, Executive Order 14178 on "Strengthening American Leadership in Digital Financial Technology."

DATES: Comments must be received on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Please submit comments electronically via the Federal eRulemaking Portal: *www.regulations.gov*. Follow the "Submit a comment" instructions. If you are reading this document on federalregister.gov, you may use the green "SUBMIT A PUBLIC COMMENT" button beneath this notice's title to submit a comment to the regulations.gov docket.

Do not include any personally identifiable information (such as name, address, or other contact information) or confidential business information that you do not want publicly disclosed. All comments are public records; they are publicly displayed exactly as received, and will not be deleted, modified, or redacted. Comments may be submitted anonymously.

Follow the search instructions on *https://www.regulations.gov* to view public comments.

FOR FURTHER INFORMATION CONTACT: Julie Lascar, Director, Office of Strategic Policy, Terrorist Financing and Financial Crimes, innovationdigitalassetsrfc@treasury.gov.

SUPPLEMENTARY INFORMATION:

I. Background

On July 18, 2025, President Trump signed into law the GENIUS Act,[1] which creates a comprehensive regulatory framework for payment stablecoin issuers in the United States. The GENIUS Act prioritizes consumer protection, strengthens the U.S. dollar's reserve currency status, and bolsters U.S. national security. It creates strong reserve requirements, aligns state and federal stablecoin frameworks, and requires clear and conspicuous redemption procedures, among other key provisions. It requires permitted payment stablecoin issuers to be treated as financial institutions for purposes of the Bank Secrecy Act, and as such, "be subject to all federal laws applicable to financial institutions located in the United States relating to economic sanctions, prevention of money laundering, customer identification, and due diligence."[2] The GENIUS Act also directs the Secretary of the Treasury to seek public comment on innovative or novel methods, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity involving digital assets.[3]

The digital asset industry plays a crucial role in innovation and economic development in the United States, and in our Nation's international leadership. On January 23, 2025, President Trump signed Executive Order 14178, "Strengthening American Leadership in Digital Financial Technology," which aims to support the responsible growth and use of digital assets, blockchain technology, and related technologies.[4] It also established the President's Working Group (Working Group) on Digital Asset Markets to strengthen U.S. leadership in digital finance.[5] The Working Group was tasked to prepare a report for the President within 180 days with recommendations for regulatory and legislative proposals that advance policies identified in the

---

[1] Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act, Pub. L. No. 119-27, 139 Stat. 419 (2025).
[2] GENIUS Act, section 4(a)(5) (Treatment Under the Bank Secrecy Act and Sanctions Laws).
[3] GENIUS Act, Pub. L. No. 119-27, 139 Stat. 419, at Sec. 9(a).
[4] Exec. Order 14178, 90 FR 8647 (Jan. 31, 2025).
[5] *Id.* at 8648.

order.[6] The Working Group's report, which was published on July 30, 2025, includes recommendations related to countering illicit finance and promoting a transparent and resilient digital asset ecosystem.[7] In addition to recommendations to improve the U.S. anti-money laundering/countering the financing of terrorism (AML/CFT) and sanctions frameworks, the report proposes that the U.S. government evaluate and consider issuing guidance on the use of digital identity verification by financial institutions and increase public-private cooperation and information sharing, including through FinCEN's 314(a) and 314(b) programs.

II. Request for Comment Overview

The GENIUS Act directs the Secretary of the Treasury to seek public comment to identify innovative or novel methods, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity, such as money laundering, involving digital assets.[8] Consistent with the GENIUS Act, following receipt of public comments, the Department of the Treasury (Treasury) will conduct research on the methods, techniques, or strategies identified in comments; submit a report that, *inter alia*, summarizes the research and provides to the chairs and ranking members of the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives legislative and regulatory proposals to allow financial institutions to develop and implement novel methods, techniques, or strategies; and issue guidance or notice and comment rulemaking based, in part, on the research results arising from comments.

The GENIUS Act lists four specific technologies on which Treasury should seek comment: application program interfaces (APIs), artificial intelligence (AI), digital identity

---

[6] *Id.*

[7] White House, *Strengthening American Leadership in Digital Financial Technology* (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

[8] The GENIUS Act defines the term "digital asset" to mean "any digital representation of value that is recorded on a cryptographically secured distributed ledger." GENIUS Act, section 2(6) (Definitions). The GENIUS Act states that the term "distributed ledger" means "technology in which data is shared across a network that creates a public digital ledger of verified transactions or information among network participants and cryptography is used to link the data to maintain the integrity of the public ledger and execute other functions." GENIUS Act, section 2(8).

verification, and use of blockchain technology and monitoring.[9] Consistent with the GENIUS Act, when conducting research on these and other innovative or novel methods, techniques, or strategies, Treasury will evaluate and consider: (a) improvements in the ability of financial institutions to detect illicit activity involving digital assets; (b) costs to regulated financial institutions; (c) the amount and sensitivity of information that is collected or reviewed; (d) privacy risk associated with the information that is collected or reviewed; (e) operational challenges and efficiency considerations; (f) cybersecurity risks; (g) and effectiveness of the methods, techniques, or strategies at mitigating illicit finance.[10]

Application Program Interfaces: APIs are a system access point or library function that allow different software applications to communicate and interact with each other, including internal and external applications.[11] This can include various applications used by a financial institution for AML/CFT and sanctions compliance. APIs can be used to share data automatically and facilitate access to transaction information. Once deployed, they can also be used to help enforce strict access controls, monitor transactions and activities, and bolster security and integrity of financial institutions providing digital asset services.

Artificial Intelligence: As used in this notice, the term AI means a "machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments."[12] The Trump Administration is prioritizing AI as a cornerstone of innovation, as outlined in the July 23, 2025, "Winning the Race: America's AI Action Plan."[13] At financial institutions, AI is playing an increasing role in AML/CFT and sanctions compliance, offering innovative solutions to help

---

[9] GENIUS Act, section 9(a) (Anti-Money Laundering Innovation).
[10] GENIUS Act, section 9(b).
[11] *See generally* National Institute of Standards and Technology (NIST), *Securing Web Transactions TLS Server Certificate Management* (June 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-16.pdf, p. 54.
[12] Exec. Order 14179, 90 FR 8741 (Jan. 31, 2025); 15 U.S.C. 9401(3).
[13] White House, *Winning the Race: America's AI Action Plan* (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf.

financial institutions analyze significant amounts of data and more effectively identify illicit finance patterns, risks, trends, and typologies.[14]

Digital Identity Verification: Digital identity verification (also known as identity proofing) is the process of establishing and verifying that a person is who they claim to be in a digital context.[15] Treasury is aware of several efforts in the digital asset industry to develop portable digital identity credentials designed to support various elements of AML/CFT and sanctions compliance, maximize user privacy, and reduce compliance burden on financial institutions.[16] These tools can incorporate different pieces of information, such as government-issued identity documents or biometrics, and can vary by operational models, governance, and convenience. Digital identity verification tools can also potentially be used by regulated digital asset intermediaries to support onboarding or by decentralized finance (DeFi) services' smart contracts to automatically check for a credential before executing a user's transaction.

Blockchain Technology and Monitoring: Many digital assets operate on public blockchains, enabling any person with access to the internet to view the pseudonymous transaction on the blockchain's public ledger.[17] Blockchain monitoring refers to the process of observing, tracking, and analyzing public blockchain data. The U.S. government, like many financial institutions offering services in digital assets, leverages public blockchain data and blockchain analytics to trace and attribute illicit activity in digital assets. Financial institutions can also use this data to evaluate high-risk counterparties and activities, analyze transactions across multiple blockchains, trace or monitor transaction activities, and identify patterns that indicate potential illicit transactions.

---

[14] For Treasury observations on use of AI, see Treasury, *2024 National Strategy for Combatting Terrorist Financing and Other Illicit Financing* (May 2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf, pp. 36-37, 89.

[15] *See generally* NIST, *Digital Identity Guidelines* (June 2017), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf, p. 2.

[16] *See generally* White House, *Strengthening American Leadership in Digital Financial Technology* (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, pp. 111-113.

[17] *See generally* Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* (Apr. 2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf, p. 32.

Innovative tools are critical to advancing AML/CFT and sanctions compliance. Financial institutions can leverage these tools to protect the digital asset ecosystem from misuse by illicit actors like drug traffickers, fraudsters, ransomware attackers, terrorist financiers, Iranian regime-linked sanctions evaders, and Democratic People's Republic of Korea (DPRK) cybercriminals. Treasury has been a leader in promoting innovation in this area over the past decade, including by championing the use of regulatory technology (RegTech) solutions to streamline compliance processes, soliciting feedback from industry on novel tools, and providing guidance and resources on new technologies.[18] Treasury is conscious, however, that innovative tools may present new resource burdens for financial institutions upon introduction due to costs to acquire and integrate new tools and to building necessary expertise. Financial institutions may also face difficulties using these tools effectively, especially at early stages of use, due to their novel nature. As such, it will be critical for financial institutions to evaluate these tools and implement them as part of a comprehensive AML/CFT and sanctions compliance program.

IV. Request for Comments

Treasury welcomes input on any matter that commenters believe is relevant to Treasury's efforts to identify and evaluate innovative or novel methods, techniques, or strategies that regulated financial institutions use to detect and mitigate illicit finance risks involving digital assets. For each method, technique, or strategy discussed in your comment, Treasury welcomes input on the following research factors that will be used to evaluate the methods, techniques, strategies, or tools: (a) improvements in ability of financial institutions to detect illicit activity involving digital assets; (b) costs to regulated financial institutions; (c) the amount and

[18] *See e.g.*, Treasury, *2024 National Strategy for Combatting Terrorist Financing and Other Illicit Financing* (May 2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf; Treasury, *Ensuring Responsible Development of Digital Assets; Request for Comment*, 87 FR 57556 (Sept. 20, 2022), https://www.federalregister.gov/documents/2022/09/20/2022-20279/ensuring-responsible-development-of-digital-assets-request-for-comment; FinCEN, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019), p. 19, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf; OFAC, *Sanctions Compliance Guidance for the Virtual Currency Industry* (Oct. 15, 2021), https://ofac.treasury.gov/media/913571/download?inline.

sensitivity of information that is collected or reviewed; (d) privacy risks associated with the information that is collected or reviewed; (e) operational challenges and efficiency considerations; (f) cybersecurity risks; and (g) effectiveness of the methods, techniques, or strategies in mitigating illicit finance.

When responding to one or more of the questions below, please note in your response the number(s) of the questions to which you are responding. When appropriate, your comment should include discussion of regulatory or statutory changes that may be necessary to effectively leverage the discussed methods, techniques, strategies, or tools. In all cases, to the extent possible, please cite any public data related to or that support your responses. If data are available, but non-public, describe such data to the extent possible.

1. In your experience, what illicit finance risks and vulnerabilities pose the greatest risk in the digital asset ecosystem? What key trends in illicit finance risks have financial institutions observed in the digital asset ecosystem?

2. What innovative or novel methods, techniques, or strategies related to APIs are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to APIs?

(a) What factors do financial institutions consider when deciding whether to employ APIs for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use APIs for these purposes, what specific compliance functions do/will APIs support? For financial institutions that decided not to use APIs, please provide additional details on the rationale for that decision.

(b) How are financial institutions using API tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible,

compare the effectiveness of API tools with other existing or previous tools used for similar purposes.

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using APIs to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of APIs for detecting illicit finance involving digital assets?

(e) Treasury will evaluate APIs and consider their impact based on the research factors identified in the GENIUS Act.[19] Provide any information pertinent to those factors.

3. What innovative or novel methods, techniques, or strategies related to AI are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to AI? Please describe the use of AI to conduct analysis of transactional data, including transactions that occur on blockchains, and to identify complex illicit financial networks, as well as key lessons learned from use of AI in this context.

(a) What factors do financial institutions consider when deciding whether to employ AI for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use AI for these purposes, what specific compliance functions does/will AI support? For financial institutions that decided not to use AI, please provide additional details on the rationale for that decision.

(b) How are financial institutions using AI tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of AI tools with other previous or existing tools used for similar purposes.

[19] GENIUS Act, section 9(b)(2).

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using AI to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of AI for detecting illicit finance involving digital assets?

(e) Treasury will evaluate AI and consider its impact based on the research factors identified in the GENIUS Act.[20] Provide any information pertinent to those factors.

4. What innovative or novel methods, techniques, or strategies related to digital identity verification are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to digital identity verification? Please describe the portable digital identity credentialing tools in use and how such tools are being used.

(a) What factors do financial institutions consider when deciding whether to employ digital identity verification for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use digital identity verification for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use digital identity verification, please provide additional details on the rationale for that decision.

(b) How are financial institutions using digital identity verification tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of digital identity tools with other existing or previous tools used for similar purposes.

[20] GENIUS Act, section 9(b)(2).

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using digital identity verification to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of digital identity verification for detecting illicit finance involving digital assets?

(e) Treasury will evaluate digital identity verification and consider its impact based on the research factors identified in the GENIUS Act.[21] Provide any information pertinent to those factors.

5. What innovative or novel methods, techniques, or strategies related to blockchain technology and monitoring are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to blockchain technology and monitoring? Please describe how financial institutions are integrating information from blockchain analytics with off-chain data and mention any key challenges associated with using blockchain analytics (e.g., obfuscation tools and methods that can complicate tracing and assessing confidence in attribution or complexities inherent in cluster analysis).

(a) What factors do financial institutions consider when deciding whether to employ blockchain technology and monitoring for AML/CFT and sanctions compliance purposes? For financial institutions that use or plan to use blockchain technology and monitoring for these purposes, what specific compliance functions does it/will it support? For financial institutions that decided not to use blockchain technology and monitoring, please provide additional details on the rationale for that decision.

(b) How are financial institutions using blockchain technology and monitoring tools in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing

[21] GENIUS Act, section 9(b)(2).

phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of blockchain technology and monitoring tools with other existing or previous tools used for similar purposes.

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using blockchain technology and monitoring to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of blockchain technology and monitoring for detecting illicit finance involving digital assets?

(e) Treasury will evaluate blockchain technology and monitoring and consider their impact based on the research factors identified in the GENIUS Act.[22] Provide any information pertinent to those factors.

6. What innovative or novel methods, techniques, or strategies related to any other innovative technologies such as cryptographic protocols and other privacy-enhancing tools, cloud-based solutions, on-chain compliance tools, oracles,[23] or new verification tools for smart contracts are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets? What are the risks, benefits, challenges, and potential safeguards related to these other innovative technologies?

(a) What factors do financial institutions consider when deciding whether to employ other innovative technologies for AML/CFT and sanctions compliance purposes? For financial institutions that decided to use or plan to use other innovative technologies for these purposes, what specific compliance functions does it/will it support? For financial

---

[22] GENIUS Act, section 9(b)(2).

[23] Oracles connect external data sources to blockchain networks. For further information, see White House, *Strengthening American Leadership in Digital Financial Technology* (July 2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf, p. 12.

institutions that decided not to use other innovative technologies for these purposes, please provide additional details on the rationale for that decision.

(b) How are financial institutions using other innovative technologies in AML/CFT and sanctions compliance efforts in relation to other tools (e.g., in testing phase while using existing tools, to augment existing tools, or to replace existing tools)? Please explain and, if possible, compare the effectiveness of other innovative technologies with other existing or previous tools used for similar purposes.

(c) Are there regulatory, legislative, supervisory, or operational obstacles to using other innovative technologies to detect illicit finance and mitigate risks involving digital assets? Please provide any recommendations related to identified obstacles.

(d) What steps, if any, should the U.S. government take to further facilitate effective, risk-based adoption of other innovative technologies for detecting illicit finance involving digital assets?

(e) Treasury will evaluate other innovative technologies and consider their impact based on the research factors identified in the GENIUS Act.[24] Provide any information pertinent to those factors.

Rachel Miller,

Executive Secretary.

[FR Doc. 2025-15697 Filed: 8/15/2025 8:45 am; Publication Date: 8/18/2025]

[24] GENIUS Act, section 9(b)(2).