Zero One Strategies

ANALYSIS

PRESIDENT'S WORKING GROUP ON DIGITAL ASSET MARKETS

Countering Illicit Finance

AUGUST 2025

Stacey Rolland
www.ZeroOneStrategies.com

The President's Working Group on Digital Asset Markets (PWG) was established by Executive Order 14178, Strengthening American Leadership in Digital Financial Technology[1], and directed to submit a report to the President within 180 days recommending regulatory and legislative proposals to support responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy. The PWG report[2] on Strengthening American Leadership in Digital Financial Technology, released July 30, 2025, proposes recommendations related to market structure, banking, stablecoins and payments, countering illicit finance, and taxation.

The below analysis focuses on the PWG recommendations for digital asset guidance and legislation on countering illicit finance, with particular focus on anti-money laundering (AML), countering the financing of terrorism (CFT), sanctions, and cybersecurity frameworks in the digital asset ecosystem.

Context and Scope

The PWG report discusses that digital assets, like other financial instruments, are subject to abuse by bad actors such as terrorists, hackers, fraudsters, sanctions evaders, and organized crime. However, their underlying technology also offers novel opportunities for risk mitigation and transparency. The report arises in the context of a shifting U.S. regulatory environment that aims to encourage innovation while safeguarding the financial system and individual privacy.

Illicit Finance Risks

Prevalence: Money laundering and terrorist financing with digital assets has increased but remains significantly lower than such activity involving fiat currencies, banks, or traditional money service providers.

Scale: Industry estimates in 2023–24 suggest illicit cryptocurrency transactions accounted for only 0.34% to 0.49% ($22.3B–$32.9B) of all on-chain volume in 2023, with the vast majority of digital asset activity being legitimate.

[1] https://www.whitehouse.gov/presidential-actions/2025/01/strengthening-american-leadership-in-digital-financial-technology/
[2] https://www.whitehouse.gov/crypto

Notable Threats: North Korea (DPRK) increasingly uses digital assets, raising national security issues, e.g., the $2.6B hack in February 2024 was the largest theft in digital asset history. Total reported fraud losses in 2024 exceeded $12B, a dramatic increase.

Vulnerabilities: Illicit actors exploit weaknesses in global AML/CFT regulation, non-compliant exchanges, anonymity-enhancing technologies (mixers, privacy coins, chain-hopping), and decentralized finance (DeFi) protocols, as well as jurisdictional arbitrage (seeking weakly regulated jurisdictions).

Current Regulatory Agencies and Frameworks

Bank Secrecy Act (BSA): The central U.S. AML/CFT law, obligating financial institutions to monitor, report, and mitigate illicit finance risks. The 2020 Anti-Money Laundering Act explicitly added digital assets to this regime.

Treasury Financial Crimes Enforcement Network (FinCEN): FinCEN has issued guidance clarifying when digital asset actors qualify as "money transmitters" and thus must comply with BSA obligations but significant uncertainties remain, especially for DeFi and purely decentralized protocols that lack a controlling administrator.

Treasury Office of Foreign Assets Control (OFAC): OFAC applies economic and trade sanctions to digital asset participants that facilitate illicit activity, with risk-based compliance expectations.

International Gaps: Global disparities in AML/CFT requirements create incentives for bad actors to use foreign, weakly regulated platforms, drawing U.S. customers away from more compliant domestic services.

Recommendation Highlights

Legislative Action

Statutory Clarity & Tailoring: Congress should define with precision which digital asset actors fall under BSA obligations and consider creating new, digital asset-specific financial institution categories. This would enable tailored AML/CFT and sanctions rules for exchanges, stablecoin issuers, and commodity traders.

Stablecoins: Require that payment stablecoin issuers are financial institutions subject to AML/CFT rules, and ensure robust secondary market surveillance and risk management.

DeFi: Congress should develop principles-based definitions to determine when DeFi actors must bear compliance obligations. Only "true" decentralized protocols (no control, no admin, no custody) might be exempt.

Global Reach: Update statutes to clarify U.S. jurisdiction over foreign-located digital asset service providers when their conduct affects U.S. interests.

Preservation of Self-Custody: Codify the principle that Americans retain the lawful right to hold and transfer their own digital assets directly, without forced intermediaries.

Clarify Software Provider Liability: Ensure that purely software-providing/non-custodial actors (who lack control over funds) are not categorized as money transmitters under the BSA.

Hold Law: Enact safe harbor laws for digital asset service providers to temporarily freeze suspected illicit funds during short investigations, with required transparency and consumer protections.

Stronger Forfeiture & Victim Compensation: Update laws and regulations to improve the government's ability to seize and forfeit digital assets used in or resulting from criminal activity, simplify victim compensation, and allow modified tracing for commingled digital assets akin to cash.

Close Legal Loopholes: Amend statutes to cover digital assets in the National Stolen Property Act and modernize anti-tip-off provisions to prevent obstructing investigations.

Regulatory Action

SAR Modernization: Treasury should update Suspicious Activity Report (SAR) forms to better capture digital asset-relevant information.

Form 8300 Alignment: Harmonize requirements for business transaction reporting of digital assets between IRS (tax) and BSA (AML/CFT) regimes.

Enhanced Public-Private Information Sharing: Expand programs (e.g., FinCEN 314(a)/(b), Illicit Virtual Asset Notification (IVAN)) for rapid intelligence sharing across traditional/digital institutions and law enforcement while respecting civil liberties.

International Cooperation: Encourage global AML/CFT framework harmonization to limit regulatory arbitrage.

Regulator Expertise: Supervisory agencies need expanded digital asset expertise, improved compliance tools, and updated examination manuals.

OFAC Authority Expansion: Allow Treasury to block specific "transmittals of funds" (not just accounts) to target foreign exchanges and non-bank/DeFi actors.

Sanctions Tools: Maintain flexibility for both full blocking and targeted sanctions on foreign digital asset firms facilitating illicit activity.

Cybersecurity in the Digital Asset Sector

Growing Threat: Nation-state actors, especially DPRK, use sophisticated social engineering and technical exploits to steal digital assets, often at immense scale.

Industry-Wide Gaps: There are insufficient mandatory cybersecurity requirements or audits. Key risks involve custody (private key theft), smart contracts (code defects), and blockchain validation.

Government Initiatives: Treasury's OCCIP is working to integrate digital asset firms into cyber-threat intelligence sharing (ATIF) and strengthen public-private coordination.

Key Recommendations:

- Implement risk-based policies for asset management, access control, secure key management, and multi-factor authentication.
- For smart contracts, adopt secure coding, third-party audits, monitoring, and deploy circuit breakers (emergency stops).
- Expand cybersecurity knowledge and information sharing across industry and with regulators.

Detailed Priorities and Recommendations

Regulatory Recommendations for Treasury Action	
Prescribe BSA Obligations	Implement the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS) which requires Treasury to adopt rules to treat permitted payment stablecoin issuers as financial institutions under the BSA and to seek public comment on strategies regulated financial institutions can use to detect illicit activity involving digital assets.
	Advance rulemaking concerning CVC mixing.
Enhance Effective Supervision	Identify areas of uncertainty for traditional financial institutions providing services to digital asset actors and services to customers and provide guidance to clarify AML/CFT obligations and expectations.
	Evaluate whether additional compliance tools, training, and resources are needed to ensure examiners can evaluate institutions' digital asset-related policies, procedures, and programs.
Adapt BSA Reporting	Evaluate modernizing Suspicious Activity Reports (SARs) to ensure it captures highly useful information.
Improve Sanctions Compliance	Issue a Request for Information (RFI) to directly solicit sanctions compliance information, input, and recommendations from industry participants to understand gaps in existing OFAC guidance and identify opportunities for enhanced private sector collaboration. Using information collected from the RFI, OFAC's existing brochure on sanctions compliance should be updated.
Increase Public-Private Cooperation	Encourage greater information sharing through domestic and cross-border information sharing programs and between digital asset and traditional financial institutions.

Apply Treasury Authorities to Digital Asset Ecosystem	Use OFAC sanctions authorities to target malicious actors and limit access of malign foreign digital asset actors to U.S. markets.

Legislative Recommendations for Congressional Action	
Prescribe BSA Obligations	Consider creating digital asset specific financial institution types within the BSA as part of market structure legislation.
	Pass legislation specifying actors within the decentralized finance ecosystem that should have AML/CFT obligations.
	Consider clarifying language regarding the BSA's application to foreign-located actors.
	Evaluate self-custody language included in CLARITY and codify principles that reinforce the importance of self-custody: - Principle 1: The importance of U.S. individuals maintaining the capability to lawfully hold their own digital assets without a financial intermediary. - Principle 2: The importance of enabling U.S. individuals to engage in lawful, direct digital asset transfers that do not involve a financial intermediary with another individual that lawfully self-custodies digital assets.
	Codify principles regarding how control over an asset impacts BSA obligations, particularly for money transmitters, through legislation such as the Blockchain Regulatory Certainty Act. Legislation should codify that a software provider that does not maintain total independent control over value is not engaged in money transmission for purpose of the BSA.

Adapt BSA Reporting	Pass legislation to ensure information required to be reported to FinCEN for BSA purposes conforms with information required to be reported to the IRS for purposes of Section 6050I.
Enable Private Sector Investigations	Enact digital asset-specific "hold law" that provides a safe harbor to institutions that temporarily and voluntarily hold property involved in suspected illegal activity during a short duration investigation, including transparency and consumer protections.
Apply Treasury Authorities to Digital Asset Ecosystem	Add a sixth special measure to Section 311 authorizing FinCEN to prohibit or impose conditions on certain "transmittal of funds" that are not tied to a correspondent banking relationship, allowing Treasury to target foreign digital asset exchanges or transactions involving criminal or state actors.
Tailor Law Enforcement Capabilities and Authorities	Evaluate victim compensation regulations and propose amendments to address concerns and improve asset forfeiture.
	Tailor 18 USC Section 1014 to protect all financial institutions, including those offering digital asset services, clarify the law applies to all false statements in connection with obtaining or maintaining access to services, and update U.S.S.G. Section 2B1.1 to include a sentencing enhancement for making false statements to financial institutions where the scheme involves significant volume of criminal funds but no loss to the institution.
	Amend the NSPA to clarify that digital assets are property.
	Amend the anti-tip-off provision in 18 U.S.C. Section 1510 to update the definition of "financial institution" to the definition in the BSA and to cover digital asset firms that operate as money services businesses, and to include additional serious underlying offences to prohibit agents of financial institutions from tipping off suspects.

	Amend 18 U.S.C. Section 984 to make certain digital assets subject to the same modified traceability requirement as exists for cash to allow the government to seize and forfeit digital assets found in the same wallet used to hold crime-linked digital assets, without requiring the government to prove the forfeited assets were the exact same digital assets derived from or used to commit a criminal offense.