

119TH CONGRESS  
2D SESSION

# H. R. 10317

To establish requirements and oversight for digital assets in the custody  
of Federal agencies, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 8, 2026

Mr. ISSA (for himself and Mr. GOODEN) introduced the following bill; which  
was referred to the Committee on the Judiciary

---

## A BILL

To establish requirements and oversight for digital assets  
in the custody of Federal agencies, and for other purposes.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. SHORT TITLE.**

4       This Act may be cited as the “Digital Asset Inventory  
5       and Audit Act of 2026” or the “Inventory Act of 2026”.

6       **SEC. 2. DEFINITIONS.**

7       In this Act:

8               (1) **CRYPTOGRAPHIC KEY MATERIAL.**—The  
9       term “cryptographic key material” means any cryp-  
10      tographic key, private key, public key, seed phrase,

1 recovery phrase, mnemonic phrase, key share, multi-  
2 party computation share, authorization credential,  
3 digital signature credential, cryptographic param-  
4 eter, or other cryptographic information or material,  
5 whether stored in physical, electronic, digital, or  
6 other form, that is used to generate, derive, authen-  
7 ticate, recover, authorize, validate, sign, transfer, or  
8 otherwise exercise custody, ownership, or control  
9 over a cryptocurrency or other distributed ledger  
10 technology-based digital asset.

11 (2) DIGITAL ASSET.—The term “digital asset”  
12 has the meaning given to it in section 2 of the Ge-  
13 nius Act (12 U.S.C. 5901).

14 (3) DISCOVERY AND SCANNING TOOL.—The  
15 term “discovery and scanning tool” means a tech-  
16 nology software specifically designed to scan digital  
17 evidence and electronically stored information ex-  
18 tracted from computers, servers, mobile devices,  
19 cloud environments, removable media, or other dig-  
20 ital storage systems to locate, identify, validate, in-  
21 ventory, classify, and triage cryptocurrency private  
22 key material and other cryptocurrency-related arti-  
23 facts for the purpose of discovering recoverable dig-  
24 ital assets and supporting their audit, investigation,  
25 recovery, seizure, and forfeiture.

1 (4) ELECTRONICALLY STORED INFORMATION.—

2 The term “electronically stored information” means  
3 digital evidence, digital storage devices, electronic  
4 records, cloud-based data, and any other electroni-  
5 cally stored data.

6 (5) FEDERAL AGENCY.—The term “Federal  
7 agency” means any department, agency, bureau, of-  
8 fice, or component of the United States Government,  
9 including the Department of Justice, Department of  
10 the Treasury, Department of Homeland Security,  
11 Intelligence Community elements, regulatory agen-  
12 cies, and law enforcement agencies.

13 (6) WALLET MATERIAL.—The term “wallet ma-  
14 terial” means a software application, hardware de-  
15 vice, physical medium, custodial service, digital ac-  
16 count, or other technological mechanism used to  
17 generate, store, manage, secure, access, recover, or  
18 utilize digital asset cryptographic key material or  
19 other authentication credentials for the purpose of  
20 holding, accessing, transferring, receiving, or other-  
21 wise exercising custody or control over a  
22 cryptocurrency or other distributed ledger tech-  
23 nology-based digital asset. The term includes custo-  
24 dial wallets, non-custodial wallets, hardware wallets,  
25 software wallets, mobile wallets, web-based wallets,

1 multi-signature wallets, multi-party computation  
2 wallets, and any successor technologies that perform  
3 substantially similar functions.

4 **SEC. 3. IDENTIFICATION AND SAFEGUARDING OF DIGITAL**  
5 **ASSETS IN FEDERAL CUSTODY.**

6 (a) PROGRAM ESTABLISHMENT.—Not later than 180  
7 days after enactment of this Act, the Attorney General,  
8 in coordination with the Secretary of Homeland Security,  
9 the Secretary of the Treasury, and the Director of Na-  
10 tional Intelligence, shall issue a binding directive applica-  
11 ble to all Federal agencies that directs all Federal agencies  
12 that collect or seize electronically stored information such  
13 as digital storage devices, electronic records, and digital  
14 evidence to—

15 (1) scan such electronically stored information  
16 for high value digital assets in the form of  
17 cryptocurrency private key material;

18 (2) properly secure these assets as soon as  
19 practicable upon electronically stored information ac-  
20 quisition; and

21 (3) conduct annual audits to oversee activity  
22 logs, ensuring comprehensive discovery, documenta-  
23 tion, and secure handling and storage of all digital  
24 assets in government custody.

1 (b) SCANNING UPON SEIZURE OR FORFEITURE.—

2 For each criminal, civil, or administrative case in which  
3 a Federal agency seizes, forfeits, or otherwise acquires  
4 custody of electronically stored information, such agency  
5 shall, as soon as practicable, scan the electronically stored  
6 information for digital assets and associated cryptographic  
7 key material.

8 (c) STANDARDS AND PROTOCOLS.—The Attorney  
9 General, in consultation with the Director of the National  
10 Institute of Standards and Technology, shall develop and  
11 publish technical standards governing—

12 (1) discovery and scanning tools of electroni-  
13 cally stored information for cryptocurrency private  
14 keys and wallet material;

15 (2) secure extraction, storage, and access con-  
16 trol of cryptographic key materials;

17 (3) preservation of chain of custody and evi-  
18 dentiary integrity; and

19 (4) logging and monitoring of all access to dig-  
20 ital asset custody systems.

21 (d) TRAINING.—The Attorney General shall establish  
22 training programs for Federal law enforcement officers,  
23 digital evidence custodians, and forensic examiners re-  
24 garding digital asset discovery, handling, storage, and  
25 audit compliance.

1 **SEC. 4. ANNUAL DIGITAL ASSET AUDITS.**

2 (a) **AUDIT REQUIREMENT.**—Each Federal agency  
3 that collects, seizes, or maintains custody of electronically  
4 stored information shall conduct an annual digital asset  
5 audit to—

6 (1) identify and account for all digital assets  
7 and cryptographic materials;

8 (2) verify secure custody and access controls;

9 (3) identify any loss, unauthorized access, or  
10 procedural deficiencies; and

11 (4) document corrective actions taken.

12 (b) **REPORTING.**—Not later than 180 days after com-  
13 pletion of each annual audit, the head of each Federal  
14 agency shall submit a report to the Attorney General and  
15 the Committees on the Judiciary, Homeland Security and  
16 Governmental Affairs, Select Committee on Intelligence,  
17 and Banking of the Senate and the Committees on the  
18 Judiciary, Homeland Security, Permanent Select Com-  
19 mittee on Intelligence, and Financial Services of the  
20 House of Representatives detailing audit findings and re-  
21 mediation measures.

22 **SEC. 5. ADDITIONAL AUDIT AND OVERSIGHT AUTHORITIES.**

23 (a) **INTERNAL AND EXTERNAL AUDITS.**—In addition  
24 to audits conducted by the Comptroller General of the  
25 United States under section 7, the Inspector General of  
26 the relevant agency, in coordination with such office as

1 the Inspector General determines appropriate or such  
2 monitors as the court may appoint, shall conduct an audit  
3 on electronic devices for digital assets and associated cryp-  
4 tographic keys.

5 (b) NO LIMITATION.—Nothing in this Act shall be  
6 construed to—

7 (1) limit the authority of any Federal entity  
8 with lawful audit or oversight jurisdiction;

9 (2) authorize the collection, search, seizure, re-  
10 tention, review, disclosure or use of electronically  
11 stored information, digital assets or cryptographic  
12 private key material except as otherwise authorized  
13 by law; or

14 (3) limit or impair any right, remedy, defense,  
15 privilege, protection, suppression argument, or pro-  
16 cedural requirement otherwise available under law.

17 **SEC. 6. INTERAGENCY COORDINATION AND OVERSIGHT.**

18 The Attorney General shall convene an interagency  
19 working group to coordinate digital asset custody prac-  
20 tices, share audit findings, and develop best practices  
21 across Federal agencies.

22 **SEC. 7. COMPTROLLER GENERAL REVIEW.**

23 (a) GAO REVIEW.—Not later than 1 years after the  
24 date of enactment of this Act, and every 3 years there-  
25 after, the Comptroller General of the United States and

1 relevant Inspector General Offices shall conduct a review  
 2 of Federal agency compliance with this Act.

3 (b) REPORT TO CONGRESS.—The Comptroller Gen-  
 4 eral of the United States shall submit to Congress a report  
 5 on the review conducted under subsection (a) containing  
 6 findings and recommendations.

7 **SEC. 8. FORFEITURE FUND FUNDING AND APPROPRIA-**  
 8 **TIONS.**

9 (a) ASSET FORFEITURE FUND.—Section 524(c)(1)  
 10 of title 28, United States Code, is amended—

11 (1) in subparagraph (I), by striking “and” at  
 12 the end;

13 (2) in subparagraph (J), by striking the period  
 14 and inserting “; and”; and

15 (3) by adding at the end the following:

16 “(K) payments for the acquisition of dig-  
 17 ital forensic tools necessary to carry out the In-  
 18 ventory Act of 2026.”.

19 (b) DEPARTMENT OF TREASURY FORFEITURE  
 20 FUND.—Section 9705(a)(1) of title 31, United States  
 21 Code, is amended by adding at the end the following:

22 “(K) Payments for the acquisition of dig-  
 23 ital forensic tools necessary to carry out the In-  
 24 ventory Act of 2026.”.