

TITLE I — SHORT TITLE; FINDINGS; PURPOSE; CONSTITUTIONAL SAFEGUARD

Sec. 101. Short Title.

This Act may be cited as the “**Founders’ Promise and American Renewal Act of 2025**” or “**FPRA**.”

Sec. 102. Congressional Findings.

Congress finds that—

1. Two hundred fifty years after the Declaration of Independence, the United States still aspires to the founders’ vision of a government that is **bold in ambition, honest in stewardship, and answerable to every citizen**;
 2. Twenty-first-century complexity—especially in artificial intelligence, cloud infrastructure, biotechnology, and intertwined global supply chains—has **outpaced traditional oversight tools**, threatening public trust and fiscal integrity;
 3. Fragmented audit authorities, slow investigatory cycles, and siloed lessons-learned allow waste, fraud, abuse, and algorithmic harm to persist across agencies;
 4. Modern cryptographic ledgers, verifiable proof-of-personhood, and open-data standards now permit **tamper-evident, real-time transparency** without sacrificing privacy or due-process rights;
 5. A **National Audit Corps** that is modular, surge-capable, and continuously learning can safeguard taxpayer resources, accelerate responsible innovation, and extend the founders’ promise into a new century; and
 6. All new federal oversight powers must remain fully subject to, and protective of, the Constitution of the United States and the liberties it guarantees.
-

Sec. 103. Purpose.

The purposes of this Act are to—

1. Establish a National Audit Corps empowered to conduct rapid, technology-aware, cross-sector audits that close oversight gaps and deter misconduct;
2. Embed **immutable public ledgers, escalating penalties, and citizen participation** to rebuild and sustain public trust;
3. Require that every audit generate lessons-learned and that those lessons be **implemented government-wide**, creating an adaptive governance ecosystem;
4. Guarantee each verified citizen or qualified public-interest entity a statutory **right to petition for audits**, reinforcing the principle of government “by the people”;
5. Align oversight incentives with measurable public value through **success-dividend funding, claw-back mechanisms, and inflation-indexed remedies**; and

6. Preserve and advance the founding generation’s ideal of a Republic that is **self-correcting, liberty-protecting, and ever ready to innovate for the common good.**
-

Sec. 104. Constitutional Non-Abrogation Clause.

Nothing in this Act shall be construed to abrogate, limit, or override any right, privilege, or protection secured by the Constitution of the United States, including the Bill of Rights and all Amendments thereto.

TITLE II — DEFINITIONS

Sec. 201. Definitions.

In this Act:

1. **“Act”** means the Founders’ Promise and American Renewal Act of 2025 (FPRA).
2. **“Corps”** or **“National Audit Corps”** means the federal audit body established under Title III.
3. **“Audit”** means any examination, inspection, or review opened pursuant to this Act.
4. **“Tier-A Audit”** means an audit triggered by Thresholds T-1 through T-5, a Bio-Risk Incident, or any audit involving a High-Risk Automated System.
5. **“Tier-B Audit”** means any audit not classified as Tier-A.
6. **“High-Risk Automated System”** means any algorithmic, machine-learning, or rules-based system that (A) affects the rights, benefits, or obligations of one million or more persons in a fiscal year, or (B) influences obligations or disbursements of \$100 million or more.
7. **“Proof-of-Personhood Score”** or **“PoP Score”** means a numeric value between 0 and 1 derived from multi-layer identity attestations in accordance with Title VI § 604.
8. **“Verified Citizen”** means a natural person with a PoP Score ≥ 0.80 .
9. **“Systemic Lesson”** or **“SL”** means a lessons-learned memorandum designated *Critical* under Title V § 509.
10. **“Lessons-Learned Memorandum”** means the post-audit report required by Title IV § 404 documenting findings, root causes, and recommended systemic changes.
11. **“Bio-Risk Incident”** means any synthesis-biology, pathogen-engineering, or high-containment breach event formally designated by the Secretary of Health and Human Services or the Secretary of Defense.
12. **“Quantum-Migration Flag”** means a cryptographic-asset marker indicating preparedness for post-quantum cryptography.
13. **“Inter-Jurisdictional Audit Memorandum of Understanding”** or **“Inter-jurisdictional Audit MOU”** means a reciprocal agreement executed under Title III § 311 extending audit triggers, data access, and lessons exchange to States, Tribal Nations, or allied governments.
14. **“Citizen Oversight Portal”** or **“Portal”** means the public interface operated under Title VI for audit status, petitions, comment submission, redaction appeals, and reauthorization consultation.

15. **“Open Audit Ledger”** means the immutable, publicly accessible chain of time-stamped audit actions maintained under Title VI § 601.
16. **“Redaction Ledger”** means the immutable public log recording every page-level redaction, statutory cite, and expiration date.
17. **“Alternative Vetting Service”** means the nationwide mail-in and kiosk-based identity-verification program established under Title VI § 604(e).
18. **“Model Governance Board”** or **“MGB”** means the body created by Title IV § 405 to oversee AI models used by the Corps.
19. **“Oversight Panel”** means the nine-member supervisory body described in Title V that resolves escalations, approves expansions, and oversees redaction appeals.
20. **“Citizen Member”** means the civil-society transparency expert serving on the Oversight Panel under Title V § 502.
21. **“Contempt Penalty Schedule”** means the escalating daily financial penalties set forth in Title VII § 702, indexed annually to CPI-U.
22. **“CPI-U”** means the Consumer Price Index for All Urban Consumers, U.S. City Average, All Items, not seasonally adjusted, as published by the Bureau of Labor Statistics.
23. **“Agency”** means any executive department, military department, government corporation, government-controlled corporation, or independent regulatory agency of the Federal Government.
24. **“Vendor”** means any private-sector entity that enters into a contract, grant, cooperative agreement, or other arrangement to provide goods or services to the Federal Government or to handle federal information.
25. **“Random-Draw Audit”** means an audit initiated under Trigger T-6, selecting not less than two percent of agencies each quarter by cryptographically seeded random process.
26. **“Success-Dividend”** means the share of recovered or avoided funds that is credited to the Corps Revolving Fund under Title VII § 704.
27. **“Week”** means five (5) business days for all statutory clocks unless expressly stated otherwise.

Any term not defined herein but defined in 44 U.S.C. § 3502, the Federal Information Security Modernization Act, or NIST Special Publication 800-37 (Revision 2) shall bear the meaning given in those provisions unless inconsistent with this Act.

TITLE III — NATIONAL AUDIT CORPS AUTHORITY & MANDATE

Sec. 301. Establishment and Independence.

- (a) There is established in the legislative branch a **National Audit Corps** (“Corps”).
- (b) The Corps is **operationally independent** of any executive-branch entity, Inspector General, or the Government Accountability Office (GAO).
- (c) The Corps is authorized to—
 - (1) initiate, conduct, and publish audits as prescribed in this Act;
 - (2) compel production of records, algorithms, logs, and other information, consistent with constitutional and statutory limits;

- (3) enter into **Inter-jurisdictional Audit MOUs** under § 311; and
 - (4) promulgate rules, after notice-and-comment, necessary to carry out its duties.
-

Sec. 302. Organization and Surge Reserve.

- (a) Sector teams: Technology, Health & Bio-Risk, Defense & Cyber, Grants & Finance, Infrastructure, and Miscellaneous.
 - (b) **Surge Reserve:** ≥ 20 percent of total auditor billets; auto-activates when live utilization exceeds 80 percent for five consecutive business days.
 - (c) Auditors rotate sectors at intervals not exceeding eighteen months.
-

Sec. 303. Statutory Audit Triggers (Non-Discretionary).

Trigger ID	Condition (any)	Initial Tier	SLA to Open
T-1	FY obligation \geq \$5 B (CPI-U indexed)	A	5 days
T-2	Deployment or material change of a High-Risk Automated System	A	48 h
T-3	Budget variance ≥ 25 % or schedule slip ≥ 6 months on a Major Acquisition	B	72 h
T-4	Cyber incident rated “High” (CISA score ≥ 8.0)	A	24 h
T-5	Bio-Risk Incident (Sec. 310)	A	24 h
T-6	Random draw — 2 % of agencies each quarter	B	5 days

Cryptographic Transparency for T-6. — T-6 audits shall be selected by a **cryptographically-seeded, open-source random process**. The random-seed value and full selection code shall be published on the Citizen Oversight Portal within 24 hours of each quarterly draw.

Failure to meet any SLA escalates automatically to the Oversight Panel and is logged on the Open Audit Ledger.

Sec. 304. Audit Categories and Timelines.

- (a) **Tier-A audits:** fieldwork plus draft findings ≤ 90 days.
- (b) **Tier-B audits:** fieldwork plus draft findings ≤ 45 days.
- (c) One extension ≤ 15 percent may be granted by Oversight Panel vote and is logged publicly.
- (d) Tier-A audits involving High-Risk Automated Systems require GAO shadow-model validation.

Sec. 305. Standard Audit Workflow.

Within seven days of opening an audit, the Corps shall—

- (1) complete a zero-knowledge conflict-of-interest scan;
- (2) assign a Lead and Deputy from different sectors; and
- (3) hold a Scoping Conference with relevant entities.

Daily hash logging, weekly peer QA, single seven-day agency rebuttal, redaction controls (Title VI), and publication follow Corps regulations.

Sec. 306. Data-Access Authority and Vendor Compliance.

(a) Agencies, vendors, grant recipients, and **FedRAMP High** cloud providers shall grant read-only forensic access within five business days of notice.

(b) Non-compliance incurs escalating penalties set in Title VII § 702; upon reaching the earlier of **1 %** of prior-year contract value or **\$25 M**, the Corps must petition for injunctive relief.

Sec. 307. Right-to-Audit Petition Process.

(a) Verified Citizens (PoP ≥ 0.80) or 501(c)(3) public-interest entities may file one petition per program per year; filing fee \$50 (CPI-U; waiver available).

(b) Corps must accept or deny within 72 hours; denials are appealable under Title V.

(c) Citizen-initiated audits consume no more than **10 %** of Corps labor-hours per FY unless backlog $< 5 \%$; Panel may raise cap to 15 %.

Sec. 308. Capacity Management and Surge Escalation.

(a) Surge Reserve activates when > 10 open audits are overdue by > 30 days.

(b) Persistent backlog after Surge may be met with external audit contracts up to 10 percent of billets.

Sec. 309. Small-Agency Relief.

Agencies with appropriations $< \$200$ M receive doubled SLAs on first breach; second breach reverts to defaults and triggers GSA surge assistance.

Sec. 310. Bio-Risk Incident Trigger.

Declaration of a **Bio-Risk Incident** by HHS or DoD automatically opens a Tier-A audit with full data-parity obligations.

Sec. 311. Inter-Jurisdictional Audit MOUs.

- (a) Corps may execute MOUs with States, Tribal Nations, or allied governments extending triggers, data-access, and lessons exchange.
 - (b) MOUs post publicly within 14 days and include a 12-month wind-down clause for withdrawal.
-

Sec. 312. Oversight Escalation.

Missed SLAs, unresolved conflicts, or redaction-cap overruns escalate to the Oversight Panel within 24 hours; status is logged on the Open Ledger.

Sec. 313. Phased Expansion Authority.

- (a) Corps billets may rise to **1 250** when GAO certifies $\geq 3\times$ ROI.
 - (b) Billets may rise to **4 000** when GAO certifies $\geq 5\times$ ROI.
 - (c) Head-count above 4 000 requires new Act of Congress.
 - (d) Expansion Impact Statement posts 30 days before billets increase.
-

Sec. 314. Crisis Descale Protocol.

- (a) Descale triggers after (1) shutdown > 14 days or (2) OMB rescission $\geq 5\%$.
 - (b) Tier-A continues; Tier-B/random-draw paused ≤ 180 days; 5 % labor reserved for citizen petitions.
 - (c) Descale status posts within 48 hours and updates monthly until normal ops resume.
-

TITLE IV — TRAINING, CERTIFICATION, AND CONTINUING-EDUCATION TRACKS

Sec. 401. Corps Training Division.

- (a) A **Training Division** is established within the Corps and led by a Senior Executive Service (SES) Director.
- (b) The Division designs, delivers, and **updates every quarter** all training, certification, and cross-sector-exchange programs required by this Act.
- (c) All federally funded curricula, assessments, and courseware are released under an open-source license and posted on the Citizen Oversight Portal.
-

Sec. 402. Baseline Audit Curriculum and Certification Tiers.

- (a) A **Baseline Audit Curriculum (BAC)** covering constitutional limits, PoP protocols, cloud forensics, AI oversight, bio-risk analysis, data-privacy law, redaction rules, and ethics must be completed by all auditors before assignment.
- (b) Certification tiers:

Tier	Eligibility	Authority	Renewal
Level 1	BAC completed	Participate in Tier-B audits	1 year
Level 2	Level 1 + 1 year experience + advanced module	Lead Tier-B; Deputy Tier-A	2 years
Level 3	Level 2 + AI & Cyber-Forensics credential + peer endorsement	Lead Tier-A audits	2 years

Sec. 403. Annual Re-Certification & Continuing Education.

- (a) Each auditor must pass an **Annual Re-Certification Assessment**; completion is logged to the Open Audit Ledger.
- (b) An auditor who misses the deadline is barred from audit duty until certified.
-

Sec. 404. Lessons-Learned Integration and Public Digest.

- (a) The Training Division shall integrate every **Critical Systemic Lesson (SL)** into curricula **no later than the first scheduled quarterly update** after SL designation.
- (b) Failure to integrate an SL within one update cycle triggers a **five-percent Training-Division budget sequester** until the Oversight Panel certifies compliance.
- (c) **Quarterly Lessons-Learned Digest.**—Not later than 30 days after each quarterly update, the Division shall publish a digest summarizing curriculum changes, SL integrations, and action items.
- (d) **Stakeholder Feedback.**—Concurrently with each digest, the Division shall open a 30-day

public-comment window via the Citizen Portal; all substantive feedback and Division responses are appended to the next digest.

Sec. 405. Cross-Sector Secondment Program.

At least ten percent of Corps personnel each fiscal year shall complete a secondment of ≥ 90 days in another federal or state audit body, accredited research lab, or allied audit entity pursuant to an Inter-Jurisdictional Audit MOU. Completion is recorded in the auditor's public credential profile.

Sec. 406. Model Governance Board (MGB).

- (a) Composition: two Corps AI leads, one GAO analytics representative, one CISA representative, and two external machine-learning researchers selected by the Oversight Panel.
 - (b) Duties: approve model deployments, publish model cards, maintain reproducible-build pipelines, and schedule retraining at least annually.
 - (c) Shadow-model validation is required for all Tier-A audits involving High-Risk Automated Systems.
-

Sec. 407. Tech Guard Pay Band & Talent Retention.

- (a) The Corps may compensate technical staff performing AI, cyber-forensics, or ledger-security roles at rates up to **Executive Schedule II** (inflation-indexed).
 - (b) Student-loan repayment and a blind-trust program are authorized to mitigate equity conflicts for private-sector recruits.
 - (c) Corps employees retain full whistleblower protections provided in Title VI § 611.
-

Sec. 408. Direct-Hire Emergency Authority.

If Corps vacancies exceed **20 percent** of authorized billets for 60 consecutive days, the Chief Executive may exercise direct-hire authority for critical positions for up to 12 months or until the vacancy rate falls below ten percent.

Sec. 409. External Partnerships & Open Courseware.

- (a) The Division may contract with accredited universities, community colleges, or nonprofit civic-tech organizations to co-develop or deliver modules.
 - (b) All deliverables funded under this subsection are published under Creative Commons Attribution 4.0.
-

Sec. 410. Funding & Reporting.

- (a) Up to **four percent** of the Corps’ annual appropriation is reserved for training, curriculum development, secondments, and talent-retention programs.
 - (b) The Division shall submit an **Annual Learning Report** to the Oversight Panel and GAO detailing—
 - (1) certification completion percentages;
 - (2) secondment statistics;
 - (3) quarterly digest metrics and SL integrations;
 - (4) vacancy and retention figures;
 - (5) Tech-Guard pay-band utilization.
-

Sec. 411. Compliance & Enforcement.

- (a) An audit led by an uncertified individual is invalid ab initio; a replacement team is assigned and statutory clocks reset.
 - (b) Two consecutive quarterly budget sequesters under § 404(b) trigger automatic review by the National Oversight Crisis Board.
-

TITLE V — OVERSIGHT, GOVERNANCE, AND REVIEW BODIES

Sec. 501. Oversight Panel Establishment.

- (a) A **nine-member Oversight Panel** (“Panel”) is constituted.
- (b) **Appointments (five-year terms):**
 - (1) Two by the Speaker of the House (majority).
 - (2) Two by the joint minority leaders.
 - (3) Two by the President pro tempore of the Senate (majority).
 - (4) One GAO designee.
 - (5) One state-level auditor elected by the National Association of State Auditors.
 - (6) One civil-society transparency expert (“Citizen Member”) chosen by majority of the first five appointees via open application.

(c) Removal only for cause by two-thirds Panel vote or court order; vacancies filled within 30 days by the original appointing authority.

Sec. 502. Quorum; Voting; Tie-Break Protocol.

- (a) **Quorum:** five members.
 - (b) Actions require majority of quorum.
 - (c) **Tie-Break:**
 - (1) If vote is tied, both the GAO designee and Citizen Member cast tiebreak votes.
 - (2) If tie persists, the **Citizen Member's vote prevails.**
 - (d) Votes, rationales, recusals, and dissents post to the Citizen Oversight Portal within 24 hours.
-

Sec. 503. Panel Powers and Duties.

- (1) Approve or deny redaction requests > 5 percent and any extension;
 - (2) Grant single audit-timeline extensions ≤ 15 percent;
 - (3) Resolve escalations under Title III § 312;
 - (4) Approve Corps phased expansions under § 313;
 - (5) Concur in Crisis-Descale activation/termination;
 - (6) Publish quarterly dashboards of decisions, penalties, and systemic-lesson adoption.
-

Sec. 504. Citizen Oversight Jury Audit.

- (a) When the GAO designee and Citizen Member vote identically and prevail on transparency, redaction, or penalty matters, a **Citizen Oversight Jury** of 25 Verified Citizens (PoP ≥ 0.90) is randomly drawn.
 - (b) The Jury audits the decision record and may overturn by two-thirds vote within 14 days; outcome posts publicly.
 - (c) Jurors are compensated at GS-09 daily rate.
-

Sec. 505. Redaction Review Board.

Five members: two privacy experts, one classification specialist, one investigative journalist, one citizen advocate (three-year terms, \$500/day). Three concurring votes required for redaction renewals beyond initial Panel approval; total redaction lifespan ≤ 48 months absent court order.

Sec. 506. Conflict-of-Interest and Ethics.

Annual asset disclosures; blind trust for holdings > \$50 000 in audited vendors. Two-year cooling-off period post-service.

Sec. 507. Recusal and Interim Substitution.

Conflict recusals are posted publicly; if quorum lost, interim alternates are drawn from the Redaction Review Board (state-auditor first preference).

Sec. 508. GAO Coordination and Shadow-Model Role.

GAO maintains a standing MOU (15 FTE, \$5 M/yr) for shadow-model validation, ROI certification, random audit review. GAO must certify ROI thresholds within 60 days or publish daily delay notices; House and Senate Administration Committees must hold a hearing within 30 days of lapse.

Sec. 509. Systemic Lesson Designation and Cultural Metrics.

Critical SL status may be set by Training Division; Panel may override. Corps publishes quarterly **C-Metrics** (certification, secondment, first-time leads, vacancy, Tech-Guard usage).

Sec. 510. National Oversight Crisis Board (NOCB).

Three retired Article III judges convene within 48 hours if ≥ 3 independent escalations unresolved for 14 days. NOCB may issue binding interim directives for 60 days; extensions require joint resolution. All actions post publicly.

Sec. 511. Reporting to Congress and the Public.

An **Annual Oversight Report** covering decisions, SL adoption, penalty escalations, Jury reversals, and NOCB activity is published unclassified on the Portal; classified annexes follow Title VI redaction rules.

Sec. 512. Whistleblower Liaison and Insurance.

Panel designates a Whistleblower Liaison; unauthorized identity disclosure triggers \$250 000–\$1 000 000 breach-insurance payout and fully funded private counsel.

Sec. 513. Live Participation Transparency for Public Ballots.

During any five-year re-authorization ballot or other major public consultation, the Citizen Oversight Portal shall **display live, anonymized participation statistics** in real time. The ballot is valid only if total verified turnout ≥ 10 percent of the prior presidential-year electorate.

TITLE VI — OPEN AUDIT LEDGER, CITIZEN PORTAL, AND PUBLIC-DATA STANDARDS

Sec. 601. Open Audit Ledger.

- (a) The Corps shall maintain an **immutable, append-only ledger** of all audit actions, triggers, penalties, redactions, lessons-learned designations, appeals, and vote tallies.
 - (b) Primary chain: **SHA-3-512** blocks mirrored to at least one NIST-approved public blockchain.
 - (c) Daily Merkle-tree roots are time-stamped by NIST Beacon and posted to the Citizen Portal.
-

Sec. 602. Data Integrity, Formats, and Schemas.

- (a) All datasets, model cards, and dashboards shall conform to the **Open Audit Data Schema (OADS) v1.0** or successor published by the Model Governance Board.
 - (b) Every public release includes a SHA-3 hash manifest and machine-readable provenance metadata.
 - (c) Backward-compatibility must be maintained or a migration changelog published ≥ 60 days prior to deployment.
-

Sec. 603. Citizen Oversight Portal.

- (a) Functions: petition filing, audit status, real-time penalty meter, redaction challenge, Citizen-Jury dashboard, re-authorization ballot access, and public comment threads.
- (b) Uptime SLA: **≥ 99.9 percent** quarterly.
- (c) API rate limit defaults to **100 requests/minute** per authenticated key (adjustable by rule).

Sec. 604. Proof-of-Personhood and Alternative Vetting.

- (a) PoP scores derive from multi-factor attestations (FIDO2/WebAuthn token, government digital ID, biometric liveness, network reputation, social vouch).
 - (b) **Adaptive anomaly scoring** throttles clusters exhibiting abnormal velocity or identical hardware fingerprints.
 - (c) **Alternative Vetting Service:** nationwide mail-in and public-library/kiosk enrollment for individuals lacking digital credentials; service funded from Corps appropriations.
 - (d) Quarterly PoP weight-matrix updates are published for public review.
-

Sec. 605. Bulk Data and API.

- (a) Nightly bulk exports of all non-restricted ledger data shall be made available in JSON and Parquet.
 - (b) Versioned, fully documented REST and GraphQL APIs must be maintained.
-

Sec. 606. Redaction Controls, Caps, and Auto-Sunset.

- (a) Default redaction cap: **5 percent** of total report pages; Panel may extend to **10 percent** by majority vote and concurrence of the Redaction Review Board.
 - (b) Redaction lifespan may not exceed **48 months** absent a federal court order issued within 60 days of renewal request.
 - (c) If court order is pending past 60 days, a ≤ 250 -word unclassified summary of withheld material auto-publishes.
-

Sec. 607. Transparency Resilience and DoS Mitigation.

- (a) The ledger and portal shall be mirrored across **two or more FedRAMP High clouds** with hourly replication checkpoints.
 - (b) **Static, signed fallback pages** are pre-positioned on a .gov CDN; an out-of-band **RSS feed and Matrix channel** broadcast audit notices and penalty meters when primary services are degraded.
-

Sec. 608. Post-Quantum Cryptography Migration.

- (a) Within 18 months of enactment the Corps CIO shall publish a **three-year PQ-migration roadmap** and mark all cryptographic assets with a **Quantum-Migration Flag**.
 - (b) An annual federal **PQ simulation test** validates ledger integrity.
 - (c) Ledger operations that remain non-PQ after three years shall be frozen until upgraded.
-

Sec. 609. Fallback Communication and Status Feeds.

- (a) During major outages (> 24 h) the Corps shall issue status updates every six hours via:
 - (1) .gov CDN static status page;
 - (2) RSS (Atom) feed;
 - (3) Matrix/ActivityPub broadcast with signed messages.
 - (b) Status archives are ingested into the ledger once normal operations resume.
-

Sec. 610. Adaptive Identity-Throttle Protocol.

- (a) If petition submissions from any PoP cohort exceed the 95th percentile velocity baseline, the Portal automatically:
 - (1) raises PoP threshold for new filings by 0.05;
 - (2) requires additional CAPTCHA + biometric liveness;
 - (3) logs throttle event to the ledger.
 - (b) Throttle resets after 72 hours of normal traffic.
-

Sec. 611. Whistleblower Shield and Breach Insurance.

- (a) Whistleblower data are end-to-end encrypted; decryption keys require multi-sig approval (Corps Chief + Whistleblower Liaison + independent privacy officer).
 - (b) Unauthorized disclosure of shielded identity triggers **breach insurance payout of \$250,000–\$1,000,000** and fully funded private counsel for the whistleblower.
 - (c) Breach events post to the ledger within 24 hours.
-

Sec. 612. Privacy and Differential-Privacy Safeguards.

- (a) Datasets containing < 250 records must employ differential-privacy noise budgets; privacy-loss metrics are published with each release.
 - (b) An Ethics & Equity Sub-Panel may reset noise budgets if re-identification risk exceeds 1 percent.
-

(Penalty schedule and enforcement for data-access non-compliance are located in Title VII § 702. All monetary amounts are inflation-indexed per § 702(g).)

TITLE VII — FUNDING, PENALTIES, SUCCESS-DIVIDEND, DESCALE, AND CRITICAL-CONTINUITY MECHANISMS

Sec. 701. Appropriations and Corps Revolving Fund.

(a) **Initial Seed.**—There is authorized to be appropriated **\$70 000 000** for Fiscal Year 2026 to carry out this Act.

(b) **Annual Operating Cap.**—Beginning FY 2027, total discretionary appropriations to the Corps shall not exceed **\$100 000 000** per fiscal year.

(c) **Revolving Fund.**—There is established in the Treasury a no-year **Corps Revolving Fund**. Twenty percent of every dollar recovered or avoided pursuant to Corps audits shall be deposited into the Fund until the current-year appropriation is fully offset; surplus balances remain available until expended.

Sec. 702. Contempt Penalty Schedule and Inflation Adjustment.

(a) **Daily Penalties for Data-Access Non-Compliance (indexed annually under subsection (g)):**

Days in Violation	≤ \$100,000,000 Program	\$100,000,001–\$1,000,000,000	> \$1,000,000,000
6 – 15	\$10,000/day	\$25,000/day	\$50,000/day
16 – 30	\$25,000/day	\$50,000/day	\$100,000/day
> 30	\$50,000/day + FAR referral	\$100,000/day + FAR referral	\$250,000/day + FAR referral

(b) **Ceiling.**—When cumulative fines reach the earlier of **1 percent** of the entity’s prior-year Federal contract value or **\$25 000 000**, the Corps shall petition the United States Court of Federal Claims for injunctive relief; payment of further fines no longer stays enforcement.

(c) **Escalation.**—Penalties double every seven consecutive days beyond 30 days of unresolved non-compliance.

(d) **Public Meter.**—Penalty accrual is displayed in real time on the Portal.

(e) **Debarment Referral.**—Violations exceeding 30 days are automatically referred to the Federal Acquisition Regulatory Council for suspension or debarment review.

(f) **Indexed Amounts.**—All dollar figures in this section are adjusted annually per subsection (g).

(g) **Inflation Adjustment.**—On 1 January of each year, the Corps Chief Financial Officer shall adjust all monetary amounts in this Act by the percentage change in the CPI-U for the 12-month

period ending the previous November and publish the updated amounts in the Federal Register and on the Portal not later than 15 January.

Sec. 703. Success-Dividend and Claw-Back Mechanisms.

(a) **Success-Dividend.**—Twenty percent of all audited recoveries, restitutions, or cost-avoidance certified by GAO shall credit to the Corps Revolving Fund.

(b) **Priority Use.**—Revolving-fund balances shall first offset current-year appropriations, then finance Surge Reserve activations, Tech-Guard pay differentials, and breach-insurance payouts.

(c) **Claw-Back.**—If a recovery is later reduced or overturned, the Corps shall debit the Revolving Fund accordingly.

Sec. 704. GAO Support Appropriation.

There is authorized to be appropriated to GAO **\$5 000 000** and **15 full-time equivalents** each fiscal year to execute its FPRA duties (shadow-model validation, ROI certification, and random audit review).

Sec. 705. Funding Floor and Automatic Appropriation.

(a) Annual appropriations for the Corps shall not fall below **0.005 percent of total discretionary budget authority** for that fiscal year.

(b) A rescission below the floor is unlawful unless enacted by joint resolution expressly referencing this section.

Sec. 706. Crisis Descale Working-Capital Authority.

(a) During a **Crisis Descale** under Title III § 314, the Corps may draw up to **15 percent** of unobligated Revolving-Fund balances to sustain Tier-A audits and the 5-percent citizen-petition reserve.

(b) Working-capital advances must be replenished from the next fiscal-year appropriation or first available recoveries.

Sec. 707. Breach-Insurance Reserve.

- (a) Within the Revolving Fund, the Corps shall maintain a **Breach-Insurance Sub-account** of not less than **\$10 000 000**.
 - (b) Payouts under Title VI § 611(c) are disbursed from this sub-account.
 - (c) If balances fall below \$10 000 000, the shortfall has first-call against the subsequent Success-Dividend.
-

Sec. 708. Critical-Service Continuity and Emergency Arbitration.

- (a) When escalating penalties threaten continuity of a vendor or agency designated as critical infrastructure, the Corps Chief, the Director of CISA, and an independent industry arbiter shall convene a **72-hour Emergency Arbitration Panel**.
 - (b) The Panel may impose supervised remediation, temporary step-in rights, or limited penalty suspension for up to **120 days**, provided:
 - (1) a *Continuity Playbook* escrowed under subsection (c) is activated;
 - (2) progress milestones are reported publicly every 30 days; and
 - (3) penalties resume automatically if milestones are unmet.
 - (c) **Continuity Playbook**.—All critical vendors shall maintain an escrowed operations-continuity plan retrievable by the Corps within 12 hours of notice.
-

Sec. 709. National Oversight Crisis Board Funding.

Expenses of the National Oversight Crisis Board (Title V § 510) are payable from the Corps Revolving Fund and are capped at **\$1 000 000 per activation**.

Sec. 710. Transparency of Financial Operations.

The Corps Chief Financial Officer shall publish quarterly statements for the Revolving Fund, Success-Dividend inflows, penalty receipts, breach-insurance payouts, and GAO support outlays. All statements post to the Portal in machine-readable format.

TITLE VIII — MISCELLANEOUS; EFFECTIVE DATES; SEVERABILITY

Sec. 801. Rule-Making and Implementation Timelines.

- (a) **Corps Regulations**.—Not later than **180 days after enactment**, the Corps shall publish interim final regulations necessary to implement this Act, including audit-workflow templates,

data schemas, PoP technical specifications, penalty-meter algorithms, and Crisis-Descale procedures.

(b) **GAO Procedures.**—Within the same 180-day period GAO shall issue procedures for shadow-model validation, ROI certification, and random audit review.

(c) **CISA & DHS Coordination.**—CISA shall, in coordination with the Corps, publish technical guidance for Continuity Playbooks required under Title VII § 708(c).

Sec. 802. State, Tribal, and Allied Participation.

(a) **Model MOU.**—A two-page standard Inter-Jurisdictional Audit Memorandum of Understanding is provided in **Appendix A** to this Act. Any State, federally recognized Tribe, or allied government may execute the MOU to opt into shared audit triggers and data exchange.

(b) **Cost Share.**—Participating jurisdictions shall bear **25 percent** of shared-audit costs unless otherwise negotiated.

(c) **Reciprocity Clause.**—All signatories grant the Corps data-access parity equal to their own auditors.

Sec. 803. Relationship to Other Laws.

(a) **No Diminution of Inspector-General Authority.**—Nothing in this Act shall be construed to limit or supersede the authorities of agency Inspectors General.

(b) **FOIA Harmony.**—Redaction procedures under Title VI shall be deemed a supplement to the Freedom of Information Act (5 U.S.C. § 552) and not an exemption.

(c) **Federal Information Security.**—Implementation shall comply with FISMA, FedRAMP, and any successor cybersecurity standards.

Sec. 804. International Data Transfers.

The Corps may transfer audit data to allied oversight bodies only under an Inter-Jurisdictional Audit MOU, ensuring equal or higher privacy, security, and transparency safeguards.

Sec. 805. Effective Date.

Except where a later deadline is expressly provided, this Act and all authorities herein shall take effect **180 days after the date of enactment**.

Sec. 806. Severability.

If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected.

Sec. 807. Table of Contents and Code References.

The Office of the Law Revision Counsel is authorized to make technical and conforming changes in the placement of this Act within the United States Code.

Sec. 808. Sunset and Review.

(a) **Statutory Sunset.**—Unless reauthorized by Congress, the Corps and all authorities under this Act shall terminate **ten (10) years** after the effective date.

(b) **Comprehensive Review.**—At least one year prior to the sunset date, GAO shall submit to Congress a comprehensive evaluation of the Corps’ performance, ROI, public-trust metrics, and recommendations for renewal or modification.

Sec. 809. References and Digital Object Identifiers.

Final, codified versions of this Act, its implementing regulations, and all subsequent major amendments shall be assigned persistent Digital Object Identifiers (DOIs) and posted on the Citizen Oversight Portal for scholarly and legal citation.

Appendix A — Model Inter-Jurisdictional Audit Memorandum of Understanding (“Model MOU” for States, Tribal Nations, Territories, or Allied Governments)

Prepared pursuant to FPRA § 802(a). Text is generic; bracketed fields are to be completed by each joining jurisdiction.

1. Parties

This Memorandum of Understanding (“MOU”) is made between:

- **The National Audit Corps** (“Corps”), an instrumentality of the legislative branch of the United States established under the *Founders’ Promise and American Renewal Act of 2025* (“FPRA”); and
- **[FULL LEGAL NAME OF JURISDICTION]** (“Partner Jurisdiction”), which may be a State, federally recognized Tribal Nation, U.S. territory, or allied government.

Together, “the Parties.”

2. Purpose and Scope

The purpose of this MOU is to enable the Partner Jurisdiction to participate in shared audit activities under FPRA Titles III & VI, including reciprocal data-access, adoption of statutory audit triggers T-1 through T-6, and exchange of lessons-learned (“Systemic Lessons”).

3. Definitions

Terms used herein that are defined in FPRA Title II (e.g., **Audit, High-Risk Automated System, Open Audit Ledger**) carry the same meaning unless otherwise stated.

4. Audit Triggers and Cooperation

1. The Partner Jurisdiction agrees that any program meeting FPRA triggers **T-1 through T-6**—and for which the jurisdiction is a funding, regulatory, or operational partner—may be audited jointly by the Corps.
 2. Either Party may request joint audits of additional programs by written notice.
-

5. Data-Access Parity

Each Party shall provide the other with audit data, records, and system logs at a protection level **no less stringent** than that afforded to its own auditors, subject to applicable law. Redactions will follow FPRA Title VI caps unless stricter local law applies.

6. Cost Sharing

Unless the Parties agree otherwise in writing, the Partner Jurisdiction will reimburse **25 percent** of direct costs incurred by the Corps for each joint audit. Cost-share invoices will be issued quarterly.

7. Privacy, Security, and Breach Notification

Both Parties will implement safeguards that meet or exceed FISMA, FedRAMP High, and FPRA Title VI requirements. Each Party will notify the other of any data-security breach affecting shared audit data **within 24 hours** of discovery.

8. Lessons-Learned Integration

Critical Systemic Lessons arising from joint audits shall be shared via the Corps' Open Audit Ledger and incorporated into both Parties' training curricula within **180 days**.

9. Withdrawal and Wind-Down

Either Party may withdraw by providing **12 months' written notice** to the other Party. No new joint audits will commence during the wind-down; ongoing audits will proceed to completion under this MOU.

10. Dispute Resolution

Disputes that cannot be resolved by the Parties' designated liaisons within 30 days shall be submitted to **binding arbitration by the National Oversight Crisis Board (NOCB)** as described in FPRA Title V § 510. The NOCB's interim directives are final for the duration of the proceeding.

(Alternatively, the Parties may strike this sentence and insert "U.S. Court of Federal Claims" or another forum.)

11. Sovereignty and Compliance

Nothing in this MOU shall be construed to waive the sovereignty or immunities of the Partner Jurisdiction. This MOU does not create enforceable rights in third parties.

12. Effective Date and Term

This MOU takes effect on the date of last signature and remains in force until withdrawn under Section 9.

Party	Name / Title	Office	Email / Phone
Corps	Corps Chief (or designee)	National Audit Corps	Corps-POC@audit.gov
Partner	[Partner Liaison]	[Agency / Dept.]	[email / phone]

14. Signatures

For the National Audit Corps	For [Partner Jurisdiction]
_____ Name: _____	_____ Name: _____
Title: Chief Executive, National Audit Corps	Title: _____
Date: _____	Date: _____

End of Appendix A — Model Inter-Jurisdictional Audit MOU