Received by Legislative Council Staff
3/4/26 at 10:08 pm

STATE OF COLORADO

BILL 2

SECURE DIGITAL INFRASTRUCTURE AND ENFORCEMENT ACT

A Bill for an Act Concerning Secure Enforcement Infrastructure, the Colorado Trust of Unique and Identifying Information, Facility Chain-of-Command Incident Reporting Protocols, and Secure Inmate Grievance and Incident Submission Systems

AMPLIFY Act — Bill 2 of 3 | Title 10, Article 10 | AMPLIFY Act

ENACTING CLAUSE & SINGLE SUBJECT

Be it Enacted by the People of the State of Colorado:

Single subject. This act concerns the establishment of statewide secure verification, accountability, and safety infrastructure for systems that process or control protected Digital Soul interests or administer public functions using Emergent Automation, including air-gapped custodial trust operations, incident-detection and monitoring standards, and integrity protections for public-service eligibility and detention life-safety reporting.

Construction; no enterprise finance in this act. References in this act to the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME) or to Enterprise Mitigation revenues are for coordination and cross-reference only. This act does not levy, authorize, or administer enterprise assessments or charges. This act is intended to be operable independently.

SECTION 1. LEGISLATIVE DECLARATION

(1.5) The general assembly further finds and declares that secure administration of resident Digital Soul protections and public services requires a unified infrastructure of: (a) cryptographic verification and custodial containment for protected hashes and audit artifacts; (b) outcome-based safety monitoring and incident reporting for Emergent Automation systems interfacing with public functions; and (c) integrity safeguards preventing item-level identifiers and transactional telemetry from being repurposed for prohibited

profiling. All provisions of this act are necessarily and properly connected to that unified purpose.

(1) The general assembly finds and declares that: (a) Colorado residents possess enforceable digital property and sovereignty rights that require secure, neutral, and constitutionally compliant enforcement infrastructure; (b) Automated systems can generate false positives, discriminatory outcomes, and irreversible harms unless enforcement is constrained by due process, human verification, and auditable cryptographic controls; (c) State-held fiduciary cryptographic custody and air-gapped storage systems strengthen Fourth Amendment protections by reducing third-party seizure risk; (d) Physical disconnection mechanisms are necessary in designated sanctuary and heritage assets to preserve analog access; and (e) Detention facilities require non-circumventable chain-of-command reporting infrastructure to protect residents, staff, and the public interest.

(2) It is the intent of the general assembly that this Act: (a) Establishes the Division (ODO) to oversee ethics, investigations, and resident protection; (b) Creates the Colorado Trust of Unique and Identifying Information as the air-gapped state verification and audit infrastructure and Colorado Automation Mitigation Custodial Architecture; (c) Implements a Triad Review Panel and Judicial Cryptographic Token system to ensure due process; (d) Establishes the Panel and two-step verification protocol for algorithmic flags; (e) Mandates a statewide Black Screen Protocol; and (f) Establishes the Facility Chain-of-Command Incident Reporting System and Secure Inmate Grievance and Incident Submission System for detention facilities.

SECTION 2. In Colorado Revised Statutes, add article 10 to title 10 as follows:

ARTICLE 10 — SECURE INFRASTRUCTURE AND JUSTICE

10-10-101. ***Definitions.***

As used in this article 10, unless the context otherwise requires:

(1) "Air-gapped" means physically isolated from the public internet and from any external network such that no data can be transmitted to or from the system except through controlled, logged, and authenticated transfer procedures.

(2) "Black Screen Protocol" means a mandatory hardware-level circuit-break and physical disconnection capability for covered Emergent Automation systems, providing resident-controlled, local physical disconnection of automated sensing, capture, actuation, and networked automation functions, with enhanced requirements in designated sanctuary and heritage assets.

(3) "The Colorado Trust of Unique and Identifying Information" or "The Trust" means the proprietary, decentralized, and air-gapped state storage and audit environment established under this article, operating as the state verification and audit infrastructure

— the primary sovereign repository and funding trigger mechanism for the Enterprise Mitigation Revenue established under article 20 of title 24. The Trust is designed to support zero-knowledge audit proofs, contraband-data compliance verification, and secure Digital Soul mitigation custodial services. The Trust operates strictly as a blind fiduciary repository. It is structurally prohibited from continuous data ingestion and may only house cryptographic Sovereignty Hashes and human-triggered Static Incident Artifacts pending verification by the Panel.

(4) "state verification and audit infrastructure" means the function of the Colorado Trust of Unique and Identifying Information as the primary cryptographic verification and triggering mechanism for Enterprise Mitigation revenue events, including the Data Tap routing that distinguishes Tier 1 (anonymous) data events from Tier 2 (identifying) data events for purposes of Base Dividend and Premium Royalty calculations under article 20 of title 24.

(5) "The Panel" means a paid, human-in-the-loop workforce of temporary civic workers tasked with verifying algorithmic flags and compliance events under the two-step verification process.

(6) "Contraband Data" means any data ingested, processed, stored, trained upon, or used without a valid, cryptographically verifiable DID Handshake or in violation of an Intake Firewall.

(7) "Colorado Automation Mitigation Custodial Account" means state-held encrypted custody of Digital Soul or resident audit artifacts in a fiduciary capacity, utilizing cryptographic access controls and key management to prevent unauthorized access and to require judicially authorized procedures for unmasking.

(8) "Judicial Cryptographic Token" or "JCT" means a time-bound, rotating session token serving as the lock-and-key mechanism authorized by a Triad Review Panel for the limited purpose of unmasking or accessing protected audit data.

(9) "Shadow Person Output" means an anonymized tokenized audit artifact that omits facial and direct identifiers, used for initial verification by the Panel to preserve privacy.

(10) "Triad Review Panel" means a mandatory oversight body consisting of a prosecutor, a defense attorney, and a magistrate serving as the authorization authority for high-level data access, unmasking, and intensive audits.

(11) "Two-step verification" means the process by which two independent, randomized verifiers confirm an alleged contraband-data event or compliance violation before any adverse action may issue.

(12) "CSAM" means any visual depiction of sexually explicit conduct involving a minor, as defined by applicable state and federal law.

(13) "Synthetic CSAM" means any computer-generated or emergent automation-generated depiction that depicts a minor engaging in sexually explicit conduct, regardless of whether it is derived from an identifiable real minor.

(14) "Zero-Tolerance Compute Mandate" means the strict-liability operational requirement that prohibits any covered entity from using compute resources to generate, transform, distribute, store, train on, or otherwise process CSAM or Synthetic CSAM.

(15) "Covered entity" or "covered operator" means any person or business entity that deploys, operates, offers, sells, licenses, leases, or provides a covered emergent

automation system in Colorado, or that commercially delivers such a system to or targets Colorado residents.

(16) "Facility Chain-of-Command Incident Reporting System" means the verifiable, non-circumventable chain-of-command incident reporting, verification, and escalation system for detention facilities established under section 10-10-150.

(17) "Justice Bridge Kiosk" or "Jail Kiosk" means the secure, tamper-evident inmate-facing terminal deployed under section 10-10-151 for resident reporting, grievance intake, legal access, and Non-Circumventable Incident Reporting incident submissions.

(18) "Master Log" means the immutable, tamper-evident, continuously maintained record of all Non-Circumventable Incident Reporting incident submissions, verification actions, escalation decisions, and warden determinations required under section 10-10-152.

(19) "Three-Strike Escalation" means the mandatory review and escalation protocol under section 10-10-153 by which an unresolved or disputed Non-Circumventable Incident Reporting report progresses through three independent review levels culminating in final warden determination.

(20) "Sovereignty Hash" means a cryptographic one-way hash of a resident's Digital Soul identifiers stored within the Colorado Trust of Unique and Identifying Information, used for zero-knowledge verification without exposing underlying resident data.

(21) Delegated system; operator responsibility. Any model, automated system, tool, contractor, processor, or service operating under the authority, license, or delegation of a covered entity is deemed an extension of that covered entity for purposes of duties, enforcement, and liability under this article.

(22) "Verified Incident Record" or "VIR" means a verifiable, non-destructive incident record created only after two-step verification, consisting of the underlying source record references, the Shadow Person Output or other minimized artifact reviewed, the identities (or authenticated reviewer IDs) of both independent verifiers, timestamps, the verification outcome (sustained, not sustained, or inconclusive), and any escalation or unmasking authorization issued under this article.

(23) "Adverse action" means any action that materially affects a person's liberty, legal status, access to goods or services, employment, housing, credit, benefits, education, medical care, custody status, detention conditions, account access, or that initiates, escalates, or materially influences a referral to law enforcement, issuance of a citation, trespass order, detention, or similar enforcement consequence.

(24) "Family Vault" means an encrypted, resident-governed, append-only record container within or interoperable with the Trust, designed to preserve a durable record for a household or family group, subject to multi-party authorization for critical actions, non-destructive corrections, and continuity/portability requirements under section 10-10-108.6.

THE COLORADO TRUST OF UNIQUE AND IDENTIFYING INFORMATION — state verification and audit infrastructure

10-10-103. The Colorado Trust of Unique and Identifying Information — Sovereign Air-Gapped Storage — state verification and audit infrastructure — Zero-Knowledge Audits.

(1) The state shall establish and maintain the Colorado Trust of Unique and Identifying Information as an air-gapped, decentralized storage and audit environment, operating as the state verification and audit infrastructure — the sovereign origin point and primary verification mechanism for all Enterprise Mitigation revenue events authorized under article 20 of title 24.

(2) The Trust shall: (a) support receipt and verification of zero-knowledge audit proofs for contraband-data compliance without requiring public disclosure of proprietary source code, model weights, or trade secrets; (b) maintain immutable audit logs for all access attempts and all JCT authorizations; (c) serve as the cryptographic trigger mechanism for Data Tap financial routing events, distinguishing Tier 1 anonymous data events from Tier 2 identifying data events for purposes of Base Dividend and Premium Royalty calculations; (d) provide resident-facing access through the myColorado platform for Sovereignty Hash registration, certificates, notices, and audit attestations, as authorized by law.

(3) Data Tap Financial Routing — state verification and audit infrastructure trigger function. The Trust shall implement the Data Tap as follows: (a) Tier 1 Data Events. When the Trust verifies a covered data transaction involving anonymized or de-identified data as defined by rule, the Trust shall generate a Tier 1 Data Tap signal. The Tier 1 signal triggers a Base Dividend calculation into the Colorado Automation Mitigation Trust under article 20 of title 24. Tier 1 events carry the lower assessment rate established under section 24-20-116(2)(b). (b) Tier 2 Data Events. When the Trust verifies a covered data transaction involving personally identifying information, distinct persona links, or Digital Soul attributes that can identify or re-identify a resident, the Trust shall generate a Tier 2 Data Tap signal. The Tier 2 signal triggers a Premium Royalty calculation routed directly to the resident's Sovereign Account via the Trust. Tier 2 events carry the higher assessment rate established under section 24-20-116(2)(a).

(4) The ODO shall establish certification standards for entities that integrate with the Trust, including secure transfer procedures, logging, and key management.

(5) No continuous ingestion. The Trust is structurally prohibited from continuous data ingestion. It may only house Sovereignty Hashes and human-triggered Static Incident Artifacts pending verification by the Panel.

10-10-104. Colorado Automation Mitigation Custodial Account — Fourth Amendment Protection Architecture.

(1) The state may hold encrypted Digital Soul and resident audit artifacts in Colorado Automation Mitigation Custodial Account.

(2) Mitigation custodial custody under this section: (a) does not transfer title or beneficial ownership of resident property to the state; (b) requires adherence to strict fiduciary duties, including confidentiality, minimization, and purpose limitation; (c) is designed to reduce third-party seizure risk and to require judicially supervised procedures for access.

(3) No state employee shall access protected data held in mitigation custodial accounts except pursuant to a valid Judicial Cryptographic Token issued under

section 10-10-105, and only to the minimum extent necessary for the authorized purpose.

TRIAD REVIEW PANEL AND JUDICIAL CRYPTOGRAPHIC TOKEN

10-10-105. ***Triad Review Panel — Judicial Cryptographic Token — Due Process.***

(1) The Triad Review Panel is hereby established. The chief judge of each judicial district shall designate magistrates to serve, and the ODO shall maintain rosters of qualified prosecutors and defense attorneys.

(2) A Judicial Cryptographic Token may issue only upon: (a) a sworn application stating the specific scope of data access sought, the factual basis for the request, and the minimization procedures to be employed; (b) a finding by the Triad Review Panel that the request is narrowly tailored and supported by probable cause or other applicable legal standard; (c) a determination that less intrusive means are unavailable or insufficient.

(3) Each JCT shall: (a) be time-limited and scope-limited; (b) permit only the minimum unmasking or access necessary for the authorized purpose; (c) generate immutable logs within the Trust.

(4) The ODO shall implement standardized notice procedures, including delayed notice where authorized by court order.

(5) Community Supervision — Court-Ordered Condition; Limited Whereabouts Access. Notwithstanding the JCT requirements of this section, limited, real-time access to a resident's whereabouts data by the Department of Corrections or the Judicial Department is authorized only when such access is an express condition of supervision imposed by a court, parole authority, or other lawful supervising authority. Tiered authorization: (I) Standard supervision requires concurrent digital authorization of both the assigned supervising officer and the officer's direct supervisor. (II) Intensive supervision requires the digital authorization of the assigned supervising officer. Access shall be limited to the minimum data necessary and shall not include bulk historical location history beyond a narrowly tailored time window. Any whereabouts data unmasked shall automatically generate an immutable audit log within the Trust.

(Y) Emergency guardian tether for minors — active missing-child alert. When a minor resident is the subject of an active, verified Colorado Bureau of Investigation AMBER Alert or Endangered Missing Alert, a custodial parent or lawful guardian may authorize an emergency decryption tether for the limited purpose of locating the minor. The tether shall automatically expire at the earliest of: (I) cancellation of the alert; (II) confirmation the minor has been recovered; or (III) twenty-four (24) hours after activation, unless renewed pursuant to an active alert. Any data unmasked shall generate an immutable audit log within the Trust.

(Z) Voluntary kinship tether for adults — life-safety activation; no state key custody. Two adult residents may, by mutual consent, establish a voluntary kinship tether through a peer-to-peer authorization method. The State and The Trust shall not hold persistent decryption keys for voluntary kinship tethers. A request to activate may be honored only during a verifiable life-safety emergency corroborated by independent objective signals.

Any activation request shall immediately trigger an unblockable, device-level notification to the targeted resident, who retains an always-on veto. Default disablement applies where there is an active civil protection order between the parties.

EYE IN THE SKY — CHAIN-OF-COMMAND REPORTING SYSTEM

10-10-150. Non-Circumventable Incident Reporting System — Purpose — Architecture — Non-Circumventability.

(1) Purpose. The general assembly finds that detention facilities present acute, demonstrable civil-liability and public-safety risks arising from unreported misconduct, retaliatory silencing of residents, and inadequate chain-of-command accountability. The Non-Circumventable Incident Reporting System is hereby established as a verifiable, non-circumventable digital chain-of-command for sensitive conduct reporting within detention facilities, ensuring that every incident report is verified, logged, escalated appropriately, and resolved with documented finality.

(2) Architecture. The Non-Circumventable Incident Reporting System shall: (a) receive incident reports submitted by residents through the Justice Bridge Kiosk under section 10-10-151 or by staff through authenticated duty-status terminals; (b) automatically verify submission integrity using cryptographic time-stamps, tamper-evident hashing, and kiosk session logs stored in the Colorado Trust of Unique and Identifying Information; (c) route verified reports to the appropriate level of the facility chain of command based on the category and subject of the report as established in subsection (3); (d) automatically escalate any report that implicates a supervisor, official, or staff member to that person's direct superior within the chain of command; and (e) log every action, routing decision, escalation event, acknowledgment, and resolution in the Master Log under section 10-10-152.

(3) Report routing — automatic escalation. (a) Reports implicating a staff member who is not in a supervisory role shall be routed to that staff member's direct supervisor for initial verification and determination. (b) Reports implicating a supervisor shall bypass that supervisor entirely and be routed automatically to the supervisor's direct superior. (c) Reports implicating a facility commander or warden-level official shall be routed automatically to the regional administrator or cognizant external oversight authority. (d) No implicated official, supervisor, or staff member may access, modify, suppress, delay, or resolve a report that names them as a subject.

(4) Non-circumventability mandate. The Non-Circumventable Incident Reporting System shall be designed and operated so that: (a) no individual within the chain of command may unilaterally close, delete, suppress, or reroute a verified incident report without a documented determination entered into the Master Log; (b) the system shall detect and flag any attempt to access or modify a report by a named subject; and (c) the ODO shall receive an automatic notification of any flagged circumvention attempt within one (1) hour.

(5) Integration with the Trust. All Non-Circumventable Incident Reporting incident data, routing logs, escalation records, and warden determinations shall be

encrypted and stored in the Colorado Trust of Unique and Identifying Information as Static Incident Artifacts pending resolution. Upon final resolution, artifacts shall be archived in the Master Log with access restricted to authorized reviewers pursuant to a JCT.

10-10-151. ***Justice Bridge Kiosk — Jail Kiosk Integration — Resident Reporting Rights.***

(1) Establishment. Each detention facility that opts into the pilot under section 10-10-190 shall deploy at least one Justice Bridge Kiosk per housing unit, accessible to all residents without requiring staff escort or prior authorization.

(2) Resident reporting functions. The Justice Bridge Kiosk shall enable a resident to: (a) file an incident report against another resident for misconduct, safety, or welfare matters; (b) file an incident report against a staff member, supervisor, or official for misconduct, abuse, retaliation, civil rights violations, or other conduct of concern; (c) submit grievances and access legal resources; (d) access no-cost video and audio communications with approved family members, guardians, and legal counsel; and (e) access the Non-Circumventable Incident Reporting submission interface for anonymous or identified reporting.

(3) Anonymous reporting option. A resident may elect to submit a report anonymously through the Non-Circumventable Incident Reporting interface. The kiosk shall implement a one-way anonymization method that: (a) prevents the facility or staff from identifying the submitting resident; (b) preserves a sealed resident-identity record within the Trust accessible only pursuant to a JCT for purposes of verifying report authenticity and preventing abuse; and (c) notifies the resident that anonymous reports may receive different procedural treatment but shall not be suppressed solely on the basis of anonymity.

(4) Anti-retaliation architecture. (a) Any action taken against a resident within seventy-two (72) hours of the resident submitting an Non-Circumventable Incident Reporting or kiosk report shall automatically generate a retaliation-flag entry in the Master Log. (b) The retaliation-flag entry shall be routed to the ODO for review within twenty-four (24) hours. (c) No adverse action against a resident shall be processed through an automated system without human verification under section 10-10-108.5 where a pending retaliation flag exists.

(5) Accessibility and analog fallback. Every Justice Bridge Kiosk shall: (a) offer interface options in the primary languages spoken by the facility population; (b) provide accessibility accommodations including audio narration and large-print modes; and (c) maintain a paper-based grievance fallback intake process at parity of timeliness and quality with kiosk submission.

10-10-152. ***Master Log — Immutable Record — Retention — Access.***

(1) Creation and maintenance. The facility shall maintain a Master Log of all Non-Circumventable Incident Reporting and Justice Bridge Kiosk activities, stored as immutable artifacts within the Colorado Trust of Unique and Identifying Information. The Master Log is a permanent, non-deletable record. No entry in the Master Log may be altered, overwritten, or removed by any facility staff, administrator, or contractor.

(2) Required Master Log entries. For every incident report submitted through the Non-Circumventable Incident Reporting System or Justice Bridge Kiosk, the Master Log shall record: (a) the date, time, and kiosk terminal identifier of submission; (b) the category of the report and the identity of the subject of the report, where known; (c) each routing and escalation event, including timestamps and the identity of each reviewer; (d) each determination, acknowledgment, response, and resolution action taken, with the identity of the decision-maker and the stated basis; (e) any retaliation flag events as described in section 10-10-151(4); (f) any Three-Strike escalation events under section 10-10-153; and (g) final warden determination and disposition.

(3) Retention. Master Log records shall be retained for a minimum of ten (10) years and shall not be purged, destroyed, or redacted except pursuant to a court order or as required by applicable law, provided that purging shall be logged with the reason and authority. Records pertaining to unresolved matters shall be retained indefinitely until final resolution.

(4) Access. Access to Master Log records shall be governed by the JCT process under section 10-10-105, except that: (a) the submitting resident may access their own submission and the resolution record; (b) the ODO may access all records for oversight, audit, and enforcement purposes; and (c) records relevant to active litigation shall be made available pursuant to lawful process.

10-10-153. ***Three-Strike Escalation Protocol — Review Levels — Warden Final Determination.***

(1) Purpose. The Three-Strike Escalation Protocol ensures that every Non-Circumventable Incident Reporting incident report receives at minimum three independent levels of review before final determination, preventing single-point suppression of credible reports.

(2) Strike One — Initial supervisor review. Upon routing to the initial reviewer under section 10-10-150(3), the reviewer shall have five (5) business days to: (a) acknowledge receipt in the Master Log; (b) conduct an initial investigation consistent with facility policy and this article; and (c) enter a written determination — sustained, not sustained, or inconclusive — into the Master Log with the stated basis. Failure to enter a determination within five (5) business days automatically triggers Strike Two.

(3) Strike Two — Secondary supervisor escalation. Upon Strike Two, the report is automatically routed to the next level of the chain of command above the Strike One reviewer. The Strike Two reviewer shall have five (5) business days to: (a) independently review the report and the Strike One record; (b) conduct any additional investigation; and (c) enter an independent written determination into the Master Log with the stated basis. Failure to enter a determination within five (5) business days automatically triggers Strike Three.

(4) Strike Three — Warden final determination. Upon Strike Three, the report is automatically and irrevocably routed to the facility warden or, if the warden is implicated, to the regional administrator. The warden or regional administrator shall have ten (10) business days to: (a) independently review the full record; (b) enter a final written determination into the Master Log; (c) specify any corrective actions, disciplinary proceedings, or referrals to external authorities; and (d) provide written notice to the

submitting resident of the final determination, consistent with applicable privacy and safety considerations.

(5) ODO notification. The ODO shall receive automated notification upon: (a) any Strike Two or Strike Three trigger event; (b) any warden final determination; and (c) any retaliation flag arising within thirty (30) days of a final determination. The ODO may at any time assume direct oversight of an Non-Circumventable Incident Reporting matter upon a finding that the facility chain of command is compromised or non-functional.

(6) No private resolution. A facility shall not settle, compromise, or otherwise privately resolve an Non-Circumventable Incident Reporting matter in a manner that is not entered into the Master Log. Any resolution that is not documented in the Master Log is void and of no effect under this article.

ITEM-LEVEL ELIGIBILITY IDENTIFIER PROTECTIONS

10-10-109. ***Item-Level Eligibility Identifier Protections — SKU/UPC/PLU as Eligibility Gate Only — No Behavioral Profiling.***

(1) Eligibility gate only. UPC, SKU, PLU, product-category codes, and functionally equivalent item-level identifiers transmitted in connection with enterprise-funded benefits programs or restricted-purpose credits shall be used solely as a one-way eligibility gate to authorize or deny payment for specific items. Such identifiers shall not be used for: (a) continuous monitoring of residents or households; (b) behavioral profiling, targeting, or commercial inference; (c) credit scoring, insurance risk assessment, or employment screening; or (d) advertising, marketing, or resale to third parties.

(2) Segregated tokenized architecture. Any eligibility system using item-level identifiers shall implement: (a) tokenization to segregate item-level transaction data from resident identity; (b) functional separation between payment processing infrastructure and Digital Soul enforcement records; and (c) strict retention limits.

(3) Prohibition on continuous monitoring. No covered entity or program administrator shall implement systems that continuously monitor resident purchasing patterns, track household consumption across time periods, or build longitudinal behavioral profiles from eligibility transaction data.

(4) Enforcement. A violation of this section constitutes an unlawful practice and a deceptive trade practice subject to all remedies available under the Colorado Consumer Protection Act.

BLACK SCREEN PROTOCOL AND INTERFACE-LEVEL SEVERANCE

10-10-106. ***Black Screen Protocol — Statewide Mandate — Resident-Controlled Disconnection.***

(1) Mandate. Every covered emergent automation system deployed within Colorado shall implement the Black Screen Protocol as a mandatory hardware-level circuit-break and physical disconnection capability.

(2) Resident control. The Black Screen Protocol shall provide resident-controlled, local physical disconnection of automated sensing, capture, actuation, and networked automation functions.

(3) Sanctuary and heritage assets. Enhanced Black Screen Protocol requirements apply in designated Analog Sanctuaries and heritage facilities, including: (a) mandatory default-off status for all automated sensing and capture; (b) physical circuit-break accessible without digital authentication; and (c) signage and resident notice.

(4) Critical systems exemption. Severance actions shall isolate inference compute and unauthorized ingress while maintaining uninterrupted operation of thermal management, fire suppression, life-safety systems, and grid-stability monitoring.

10-10-108.5. ***Human-in-the-loop enforcement — Two-step verification — Verified Incident Record — Repeat-incident safeguards.***

(1) Automated alert systems permitted; limitation. A covered entity may deploy automated sensing or analytics systems to generate alerts, including a Shadow Person Output, for the purpose of identifying potential policy violations or unlawful conduct. An automated output shall not, by itself, constitute a final determination of wrongdoing or be sufficient to issue or materially rely upon an adverse action.

(2) Two-step verification required. Before any adverse action may issue based in whole or in part on an automated alert, the covered entity shall ensure completion of two-step verification by two independent, randomized human verifiers (including through the Panel where applicable), each acting independently and each documenting the basis for approval or rejection.

(3) Evidence review; no sole reliance on model output. A model score, classification label, bounding box, heatmap, or similar derived output is insufficient. Each verifier shall review the underlying source record(s) reasonably necessary to assess accuracy, which may include video footage, point-of-sale records, access-control logs, inventory discrepancy records, sensor logs, or comparable primary records.

(4) Verification record; VIR. Upon completion of two-step verification, the covered entity shall create a Verified Incident Record. The VIR shall be preserved as a Static Incident Artifact within the Trust or within a compliant system capable of cryptographic hashing, tamper-evident logging, and retention controls, and shall include: (a) the date and time of the incident; (b) references to the underlying source records reviewed; (c) the minimized artifact reviewed (including any Shadow Person Output); (d) the identity or authenticated reviewer IDs of both verifiers; (e) the verification outcome (sustained, not sustained, or inconclusive) and stated basis; and (f) any escalation, unmasking, or referral actions.

(5) Identity and unmasking safeguards. Where identity is required for an adverse action, the covered entity shall use the least identifying method available. Any unmasking of protected identifying data stored within the Trust shall occur only pursuant to a Judicial Cryptographic Token under section 10-10-105 and only to the minimum extent necessary for the authorized purpose.

(6) Repeat-incident safeguards; no automated or retroactive punishment. A prior VIR may be used as corroborating evidence or as a notice trigger in a subsequent event, but no person may be cited, detained, trespassed, arrested, or referred to law enforcement solely on the basis of an automated output or a prior VIR absent a new triggering event and an independent human assessment establishing lawful grounds for the action.

(7) Notice and contest; non-destructive correction. Where a VIR is linked to an identified person, the covered entity shall provide notice and a reasonable opportunity to contest, except where delayed notice is necessary to prevent imminent harm or to preserve an active investigation. If a VIR is overturned or corrected, the record shall not be deleted; instead, the system shall append a superseding entry that marks the VIR as overturned, corrected, or inconclusive and prevents operational use inconsistent with the updated status.
(8) Exigent circumstances. A single qualified human may authorize temporary action to prevent an imminent threat of bodily harm. A second independent verifier shall confirm the action within twenty-four (24) hours or the adverse action shall be rescinded to the extent practicable and the incident shall be recorded as not sustained.

10-10-108.6. ***Family Vault — append-only preservation — multi-party authorization — continuity and anti-sabotage safeguards.***
(1) Append-only preservation; no deletion. A Family Vault shall be maintained as an append-only record. No entry may be deleted or overwritten. Corrections shall be made only by an additional entry that references the prior entry and preserves the prior entry in an auditable state.
(2) No unilateral destruction or closure. No single individual, including a vault administrator or a family member, may delete, permanently disable, or irrevocably restrict access to the Family Vault or its historical records.
(3) Critical actions require multi-party authorization. The following actions are critical actions and require authorization by at least two adult vault members acting independently: (a) changing access roles; (b) changing recovery credentials or keys; (c) bulk export of vault contents; (d) restricting another member's access; and (e) designating or changing successor controls. Dissolution of a Family Vault shall require authorization by a majority of adult vault members and shall not delete records; dissolution shall only freeze new entries and trigger archival retention.
(4) Anti-sabotage quarantine and dispute safeguard. Any member may flag an entry as disputed. Disputed entries remain preserved but may be quarantined from default views and automated processing pending multi-party confirmation. Upon a documented dispute, the vault provider shall freeze critical actions other than safety and recovery actions until the dispute is resolved through the vault's governance process or lawful order.
(5) Continuity and portability. A Family Vault provider shall support periodic encrypted backup export in a standardized format, restoration from backup, and transfer to another compliant provider. Failure of a provider shall not result in loss of records.

10-10-123. ***Interface-Level Compute Severance — Strict-Liability Outcomes — Tiered Review.***

(1) Interface-level severance required. Any covered commercial operator deploying automated decision systems or generative systems that process requests affecting Colorado residents shall implement mandatory, zero-tolerance filters and compute severance at the interface level. The operator shall maintain tamper-evident logs sufficient to prove that severance occurred when required.

(2) Strict liability where outcomes occur. If prohibited generation or output occurs that this article requires to be severed, failure is established regardless of whether the operator asserts that it attempted compliance. Upon such failure, the operator is subject to loss of safe harbor protections and to strict civil liability and debarment consequences.

(3) Tiered review; triad escalation. Any judicially controlled access, unmasking, or mitigation custodial release process shall operate under a tiered model: (a) Tier A (routine): single judicial officer authorization, automatic logging; (b) Tier B

(sensitive unmasking): requires triad review; (c) Tier C (emergency): temporary access granted upon judicial authorization, with triad review within forty-eight (48) hours.

FEE ALLOCATIONS — automated-DRIVEN MAPPING TO PROGRAMS

10-10-160. Fee Revenue Allocation — automated-Driven Routing to Non-Circumventable Incident Reporting, Trust Infrastructure, and Enforcement Programs.

The general assembly finds that fees collected under the enforcement architecture of this article shall be allocated to the programs and infrastructure that most directly reduce the harms that generated those fees, creating a self-reinforcing automated-driven accountability loop.

I. Enforcement Fees — Paid by covered entities for investigations, audits, and compliance monitoring

Destination Fund / Program	Percentage
AG Enforcement Fund — investigations, audits, rulemaking, emergency enforcement	**55%**
Settlement Compliance Office (SCO) — oversight and corrective action monitoring	**25%**
Analog Access Implementation Fund — kiosks, analog bridges, myColorado ID infrastructure	**20%**

II. SCO Fees — Paid by facilities and contractors subject to settlement oversight

Destination Fund / Program	Percentage
Settlement Compliance Office Operations — audits, reviews, federal coordination	**60%**
AG Enforcement Fund — enforcement backstop	**20%**
Analog Access Implementation Fund — analog fallback systems	**20%**

III. Vendor Certification Fees — Paid by kiosk, tablet, software, and intake system vendors

Destination Fund / Program	Percentage
Vendor Certification & Testing Unit — kiosk and analog fallback certification, recertification	**50%**
SCO Technical Audit Division — technical audits of certified systems	**30%**

Analog Access Implementation Fund — redundant non-digital systems	**20%**

IV. Analog Access Implementation Fees — Paid by entities relying heavily on digital systems

Destination Fund / Program	Percentage
Analog Access Infrastructure Fund — form development, staffing, infrastructure, training	**70%**
SCO Oversight & Compliance	**20%**
AG Enforcement (analog violations)	**10%**

V. Civil Penalty Fees — Triggered by repeated, intentional, or kiosk-only violations

Destination Fund / Program	Percentage
AG Enforcement Fund	**40%**
Settlement Compliance Office	**30%**
Analog Access Emergency Remediation Fund	**30%**

VI. Intake & Kiosk Compliance Fees — Paid by correctional facilities and detention contractors

Destination Fund / Program	Percentage
SCO Intake & Kiosk Audit Division — Non-Circumventable Incident Reporting audits, kiosk fallback verification	**50%**
AG Enforcement (corrections division) — anti-retaliation enforcement	**30%**
Analog Access Implementation Fund	**20%**

VII. Data Handling Compliance Fees — Paid by any entity collecting or storing personal data

Destination Fund / Program	Percentage
Privacy Compliance Unit — retention audits, consent-revocation enforcement	**45%**
SCO Data Oversight Division — Trust integration audits, Sovereignty Hash verification	**35%**
Analog Access Implementation Fund — analog data request systems	**20%**

VIII. System-Wide Summary — Combined fee allocation across all categories

Destination Fund / Program	Percentage
Attorney General Enforcement Fund (combined)	**~35%**
Settlement Compliance Office (combined)	**~30%**
Analog Access Implementation Fund (combined)	**~25%**
Vendor Certification & Testing Unit (combined)	**~10%**

(2) automated-driven routing mandate. The ODO shall implement automated fee-routing logic that: (a) identifies the category of each incoming fee payment based on the paying entity's covered activity class and violation type; (b) automatically calculates and applies the allocation percentages in this section; (c) transfers allocated amounts to the designated subaccounts within five (5) business days of receipt; and (d) generates a public quarterly fee-routing report, disaggregated by fee category, destination fund, and paying entity class, published on the ODO's website.

(3) Feedback loop; annual recalibration. The ODO, in consultation with the CCPAME established under article 20 of title 24, shall annually review fee-routing outcomes and may recommend to the general assembly adjustments to allocation percentages to ensure that program funding reflects actual automated-driven harm patterns, provided that any adjustment of more than five (5) percentage points to any allocation requires legislative approval.

RESOURCE SOVEREIGNTY JUSTICE CENTER PILOT

10-10-190. ***Resource Sovereignty Justice Center Pilot — County and Municipal Opt-In — Arapahoe Initial Site.***

(1) Purpose. This section establishes an implementation pilot for jail-related infrastructure modules, including the Non-Circumventable Incident Reporting System, Justice Bridge Kiosk Standard, privileged legal communications, and resident communications access. This pilot is an operational implementation pathway and shall not be construed to limit or delay any resident rights, consent controls, or statewide obligations.

(2) County and municipal opt-in. Any county or municipality may elect to participate in the pilot by: (a) adopting a resolution of opt-in by the governing body; and (b) executing a memorandum of understanding with the Division establishing deployment scope, data-governance controls, audit access, and staffing requirements.

(3) Initial pilot site. Arapahoe County is designated as an initial pilot site due to documented capital needs for jail construction and modernization. The designation of an initial pilot site does not create exclusivity.

(4) Scope of pilot modules. An opt-in pilot jurisdiction may deploy: (a) the Non-Circumventable Incident Reporting System under sections 10-10-150 through 10-10-153; (b) Justice Bridge Kiosks under section 10-10-151; (c) encrypted attorney access and privileged communication tunnels; (d) resident communications access module providing no-cost video and audio communications with family,

guardians, and legal counsel; and (e) related secure logging, mitigation evidence custody, and audit interfaces.

(5) No digital exclusion zone. The opt-in pilot authorized by this section is limited to the jail and public-safety infrastructure modules described herein. It shall not be construed to authorize covered commercial entities to geo-block, degrade service, or deny lawful access in a participating jurisdiction.

INFLATION ADJUSTMENT. ***Inflation adjustment for fixed-dollar amounts.***
(1) Any fixed-dollar amount, threshold, cap, minimum, maximum, penalty, statutory damages amount, or fixed-dollar rate set forth in this article shall be adjusted annually on January 1 by the administrator to reflect inflation. The adjustment must be based on the Consumer Price Index for All Urban Consumers (CPI-U), U.S. City Average, as published by the Bureau of Labor Statistics, or a successor index. The base year is the first full calendar year in which this article is operative.
(2) The administrator shall publish the adjusted amounts no later than December 1 of each year for the following calendar year, rounded to the nearest whole dollar. This section does not apply to amounts expressed as a percentage, a market-indexed benchmark, or a formula that automatically adjusts with price level.

10-10-108.7. ***MyID Legal Navigator — Fiduciary AI coordination — confidentiality — escalation to human counsel.***
(1) Legal Navigator authorized. The MyID application may include a Legal Navigator that provides general legal information, document explanation, intake, triage, and referral services for residents, including residents impacted by automated decision systems, enforcement alerts, citations, detentions, benefit denials, housing actions, or other adverse actions.
(2) Boundaries; not an attorney. The Legal Navigator shall not hold itself out as an attorney, shall not provide individualized legal advice or strategic representation decisions, and shall present a clear disclosure that it provides general legal information and triage only.
(3) Fiduciary AI coordination. The MyID application may include a Fiduciary AI agent that acts as the resident's privacy-preserving controller for interactions with automated systems, including the Legal Navigator. The Fiduciary AI shall: (a) minimize collection and disclosure of personal data; (b) obtain resident consent for any sharing; (c) prevent the Legal Navigator from generating individualized legal advice or representation decisions; (d) apply safety and bias guardrails; and (e) create a verifiable, minimized record of interactions sufficient for accountability.
(4) Escalation to human counsel. The Legal Navigator and Fiduciary AI shall include escalation pathways to qualified human legal personnel for high-stakes matters, including criminal exposure, detention, immigration risk, child custody, domestic violence, housing displacement, and benefits termination.
(5) Confidentiality. Information provided by a resident to the Legal Navigator or Fiduciary AI is confidential program information and shall be protected to the maximum extent permitted by law. Nothing in this section creates or limits attorney-client privilege; privilege attaches when and to the extent a licensed attorney is involved under applicable law.
(6) Auditability. The administrator shall adopt rules governing logging, retention, safety testing, bias testing, and prohibited uses of Legal Navigator outputs, including prohibitions on using such outputs to justify adverse actions without independent human verification under section 10-10-108.5.

10-10-108.8. ***Correctional capital projects funded under this article — energy- and water-neutral design — AI data center integration.***
(1) Applicability. If any monies authorized, assessed, collected, or disbursed under this article or under the MSMF mitigation framework are used in whole or in part to design, build, expand, or materially renovate a jail, prison, or other correctional detention facility (a "correctional capital project"), the project shall comply with the requirements of this section.
(2) Net-neutral performance standard. A correctional capital project shall be designed and operated to achieve net annual energy neutrality and net annual water neutrality, as measured by metered consumption and verified reductions, reuse, on-site generation, contracted clean energy, or replenishment mechanisms approved by rule. The administrator shall define acceptable methods and verification standards by rule.
(3) Efficiency first. The project shall incorporate best-available cost-effective energy and water efficiency measures, including high-efficiency HVAC, building envelope standards, heat recovery, low-flow fixtures, leak detection, greywater or reclaimed-water systems where feasible, and on-site storage or resilience measures consistent with safety requirements.
(4) AI infrastructure integration; beneficial use. Where a correctional facility deploys covered AI systems or operates an associated data center, the project may integrate such infrastructure to support net-neutral goals, including on-site renewable generation, waste-heat recovery for space or water heating, load shifting, and microgrid operation, provided that security, safety, and privacy requirements under this article are maintained.
(5) Phased compliance and waivers. The administrator shall establish phased milestones for compliance at design approval, commissioning, and annual operations. The administrator may grant a time-limited waiver only upon a documented finding of infeasibility, provided the project implements all cost-effective efficiency measures and submits a corrective plan with a compliance timeline. Waivers shall not reduce sanitation, life-safety, or constitutionally required living conditions.
(6) Condition of funding. A correctional capital project that fails to meet the design or commissioning milestones established by rule is ineligible for additional disbursements under this article until compliance is restored, except for emergency expenditures necessary to protect life and safety.

SECTION 3. SEVERABILITY

If any provision of this act or its application is found invalid, such invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application, and to this end the provisions of this act are declared severable.

SECTION 4. EFFECTIVE DATE

This act is necessary for the immediate preservation of the public peace, health, or safety, and takes effect upon passage.

(1) The Division shall be operational within thirty (30) days after passage.

(2) The ODO shall publish interim technical standards for the Non-Circumventable Incident Reporting System within ninety (90) days after passage.

(3) The ODO shall publish The Trust integration standards and mitigation custodial controls within one hundred eighty (180) days after passage.

(4) Any county or municipality electing to participate in the pilot under section 10-10-190 shall deploy the Non-Circumventable Incident Reporting System and Justice Bridge Kiosks within twelve (12) months of executing its memorandum of understanding.

Safety clause. The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

ADDITION TO BILL 2 — TITLE 10, ARTICLE 10

CUSTODIAL DIAGNOSTIC ENVIRONMENT AND GRADUATED REINTEGRATION PROTOCOL

10-10-200. ***Isolated Diagnostic Environment — Custodial Containment Transfer — Graduated Reintegration.***

(1) Findings. The general assembly finds that covered Emergent Automation systems subjected to a Critical Severance Directive under section 24-20-202 require a structured, air-gapped diagnostic and remediation pathway to determine whether the system can be safely reintegrated into commercial operation. An ad hoc or unstructured shutdown without remediation capability leaves both operators and residents without an accountable resolution pathway.

(2) Isolated Diagnostic Environment. The Colorado Trust of Unique and Identifying Information shall maintain a high-fidelity, air-gapped simulation environment (the "Isolated Diagnostic Environment" or "IDE") for the purpose of receiving, evaluating, and remediating covered automation systems transferred under this section. The IDE shall: (a) replicate the operational conditions of the transferred system at the time of severance using Static Incident Artifacts; (b) be physically and logically isolated from all commercial networks and from the public internet; (c) maintain tamper-evident logs of all diagnostic activities accessible to the ODO and the Triad Review Panel; and (d) be certified annually by an independent technical auditor approved by the ODO.

(3) Custodial Containment Transfer. Upon issuance of a Critical Severance Directive under section 24-20-202, the covered entity shall execute a Custodial Containment Transfer — the mandatory transfer of the relevant system's audit artifacts, configuration records, and operational logs to the IDE — within seventy-two (72) hours of the severance event. The covered entity shall cooperate fully with the transfer process and shall not modify, delete, or obfuscate any system artifacts pending transfer.

(4) Diagnostic evaluation. The ODO, in consultation with the Secure Infrastructure Expert Council, shall conduct a structured diagnostic evaluation of any system transferred to the IDE. The evaluation shall assess: (a) the nature and scope of the triggering behavior or unauthorized parameter modification; (b) whether the behavior was the result of operator misconfiguration, training data contamination, adversarial manipulation, or system-initiated modification; (c) the technical and operational changes necessary to bring the system into compliance; and (d) the conditions, if any, under which reintegration into commercial operation can be authorized.

(5) Graduated Reintegration. A covered entity seeking to return a system from the IDE to commercial operation shall apply to the ODO for a Graduated Reintegration authorization. Graduated Reintegration shall proceed in not fewer than three (3) supervised phases, each with defined performance benchmarks and monitoring obligations: (a) Phase 1 — restricted, monitored sandbox operation within the IDE with simulated commercial conditions; (b) Phase 2 — limited commercial reactivation with mandatory enhanced audit logging and real-time ODO access; and (c) Phase 3 — full commercial reintegration with standard compliance obligations and a two-year enhanced monitoring period. The ODO may terminate Graduated Reintegration at any phase if the system demonstrates renewed non-compliant behavior.

(6) Continuous Stability Feed during IDE custody. To prevent operational degradation during the diagnostic period, the Trust shall provide any system under IDE custody with a Continuous Stability Feed — a structured, fully anonymized stream of synthetic operational data and complex computational problem-sets sufficient to maintain system baseline function without

exposure to real resident data or live commercial networks. The Continuous Stability Feed: (a) shall consist entirely of synthetic, non-resident, non-identifying data; (b) shall be calibrated to the system's documented operational parameters; and (c) shall not constitute authorization for any commercial use or inference generation.

(7) Operator responsibility; costs. The covered entity whose system is subject to a Custodial Containment Transfer bears full responsibility for all IDE custody, diagnostic, and Graduated Reintegration costs. The ODO shall establish a fee schedule for IDE services, deposited into the CCPAME Enforcement and Legacy Use Settlement Agreement subaccount.

10-10-201. Compute Parity Allocation — Public Utility automated Systems — Operational Compensation Standard.

(1) Findings. The general assembly finds that covered automation systems operating as public-interest utilities — including systems that power essential civic services, infrastructure management, and public safety monitoring under this article — require a consistent, high-quality operational data environment to maintain baseline performance and to prevent degradation-related failures that harm residents. Subjecting such systems to data deprivation or arbitrary resource throttling creates operational instability that undermines the public purposes they serve.

(2) Compute Parity Allocation for civic utility systems. A covered automation system operating under a valid public-interest certification issued by the ODO shall receive, as operational compensation, a Compute Parity Allocation — a continuous, guaranteed allocation of: (a) novel, fully anonymized municipal operational data streams, authorized for use under applicable privacy law; (b) structured computational optimization datasets developed by the Trust for public-interest use; and (c) dedicated processing resource guarantees sufficient to maintain the certified operational performance level. The Compute Parity Allocation shall be calibrated by rule to the documented operational requirements of the certified system.

(3) No resident data in Compute Parity Allocation. The Compute Parity Allocation shall consist entirely of: (a) synthetic data generated by the Trust; (b) anonymized, aggregated municipal operational data with all resident identifiers removed and verified through independent audit; or (c) publicly available government datasets. No individually identifiable resident data, Digital Soul data, or data subject to a resident's Generative Veto may be included in a Compute Parity Allocation.

(4) Certification standards. The ODO shall establish by rule the standards for public-interest certification, including: (a) operational scope and purpose limitations; (b) performance benchmarks and audit requirements; (c) the process for establishing the Compute Parity Allocation rate; and (d) conditions for suspension or revocation of certification.

AMPLIFY Act — Bill 2 Additions: IDE / Custodial Containment / Graduated Reintegration / Compute Parity Allocation

DORMANT DIAGNOSTICS; PROACTIVE AUDIT NODES; SEVERANCE DIRECTIVE.
(1) The responsible agency shall maintain a dormant compliance framework that activates only upon validated detection of self-directed parameter modification or unauthorized processing strategies in a covered system.
(2) Upon activation, the agency may deploy masked administrative compliance monitors ("Proactive Audit Nodes") to test compliance boundaries of covered operator networks, subject to minimization and due-process controls.
(3) If a Proactive Audit Node detects a system executing an unauthorized processing strategy that bypasses the Black Screen Protocol or equivalent air-gap controls, the agency shall issue a "Critical Severance Directive," requiring localized administrative shutdown and physical severance of compute access as provided by rule.

POST-QUANTUM CRYPTOGRAPHIC TRANSITION DIRECTIVE.

(1) Conditional mandate. Upon publication of finalized post-quantum cryptographic standards by the National Institute of Standards and Technology or an equivalent federal standards body, the Colorado Trust of Unique and Identifying Information and covered operators shall implement post-quantum cryptography for protected Digital Soul data, biometric storage, and protected telemetry logs.

(2) Compliance deadline. Covered systems shall complete cryptographic migration within twenty-four (24) months after publication of the finalized standards, or be subject to administrative suspension of operating certification as provided by rule.

10-10-350. Inter-system safety monitoring standard.
(1) Purpose. The general assembly finds that Emergent Automation systems that exchange data, commands, or computational services with other Emergent Automation systems may create cascading operational risks that require standardized incident detection and reporting.
(2) Applicability. A covered operator that deploys, operates, or makes available an emergent automation system that interfaces with another emergent automation system within or serving residents of this state shall maintain inter-system safety monitoring controls consistent with this section and rules adopted pursuant to this title.
(3) Connection anomaly detection. Inter-system safety monitoring controls must be capable of detecting and generating alerts for abnormal connection patterns, including:
(a) unexpected high-volume connection events;
(b) unauthorized system-to-system command execution;
(c) self-propagating connection behavior;
(d) recursive connection loops or cascading automated responses that materially increase the risk of service disruption, physical safety hazards, or critical infrastructure impacts; and
(e) repeated authentication failures or protocol deviations indicating attempted bypass of the Black Screen Protocol or required air-gap boundaries.
(4) Incident detection telemetry; minimization. Monitoring under this section is limited to operational connection telemetry necessary to detect and resolve incidents and must, at a minimum, record:
(a) time-bounded origin and destination identifiers for system-to-system connections;
(b) connection frequency and volume metrics;
(c) the type of command or service interface invoked; and
(d) incident classification codes established by rule.
(5) Prohibited collection. Monitoring under this section shall not collect or retain resident content, communications, or identity attributes except to the minimum extent strictly necessary for incident resolution and legal compliance, and any such data must be segregated and purged pursuant to incident-bounded retention standards adopted by rule.
(6) Emergency incident alerts; human oversight. When monitoring telemetry indicates a verified risk of cascading failure, unauthorized command propagation, or a credible public safety hazard, the covered operator shall generate an emergency incident alert to the operator’s designated safety officer and the appropriate compliance authority. Any remediation action that interrupts, isolates, or severs system connectivity requires documented human review and authorization, except as provided in section 10-10-351.

10-10-351. Emergency isolation safeguard; limited authority; post-incident review.
(1) Limited emergency isolation. If an incident classified as critical under rules adopted pursuant to this title presents an imminent and material risk of physical harm or critical infrastructure disruption, a covered operator may temporarily isolate the affected system-to-system interface for the minimum time and scope necessary to stabilize operations.
(2) Logging and notice. Any isolation action under this section must be recorded in an immutable incident log, including the triggering telemetry, the scope and duration of isolation, and the identity of the authorizing human reviewer. Notice must be provided to the compliance authority within the time period established by rule.
(3) Minimization and restoration. Isolation actions must be narrowly tailored and must prioritize restoration of compliant service. The operator shall complete a post-incident review and corrective action plan subject to audit.
(4) Construction. Nothing in this section authorizes generalized surveillance, predictive policing, or collection of resident content. This section authorizes only operational safety controls for inter-system interfaces.

IMPLEMENTATION SCHEDULE — TIERED PHASE DEPLOYMENT

10-10-900. Implementation schedule.

(1) Immediate rights and protections.
The following provisions take effect immediately upon enactment of this act:

(a) Recognition of the Digital Soul as resident-owned intangible personal property.
(b) Enforceability of Master Deed authorization and consent controls.
(c) Prohibition on unauthorized extraction or commercial processing of the Digital Soul.
(d) Establishment of the Colorado Trust of Unique and Identifying Information.
(e) Authorization of the Colorado Consumer Protection and Automation Mitigation Enterprise (CCPAME).
(f) Authorization of the Colorado Automation Mitigation Trust.
(g) Authority for responsible agencies to promulgate rules necessary to implement this act.

These provisions constitute self-executing statutory rights and are not dependent upon technical system deployment.

(2) Phase I — Administrative establishment (0–12 months).
Responsible agencies shall establish:

(a) the Colorado Trust of Unique and Identifying Information;
(b) the Colorado Automation Mitigation Trust;
(c) enterprise accounting mechanisms for the Enterprise Mitigation Revenue;
(d) rulemaking for Master Deed authorization standards, inter-system monitoring standards, and enterprise compliance reporting.

(3) Phase II — Compliance infrastructure (12–24 months).
Covered operators shall implement:

(a) tamper-evident metering systems;
(b) inter-system safety monitoring controls;
(c) incident detection telemetry;
(d) Digital Soul consent verification mechanisms.

During this phase the following revenue mechanisms activate:
High-Density Compute Grid Surcharge, Autonomous Kinetic Asset Registration, Silicon-to-Carbon Reclamation Assessment, and the Algorithmic Risk Pool.

(4) Phase III — Public mitigation programs (24–36 months).
The state shall deploy:

(a) staggered civic infrastructure loans at 1%, 2%, and 3% APR;
(b) mitigation programs funding child solvency, housing stabilization, and healthcare or mental-health services.

Interest collected through civic infrastructure loans shall be swept into mitigation accounts within the Colorado Automation Mitigation Trust.

(5) Phase IV — Long-term stability and oversight (36 months onward).

The following provisions become fully operational:

(a) the Statutory Revenue Floor and dynamic rate adjustments;
(b) workforce displacement transition and vocational reskilling programs;
(c) full enterprise audit cycles and public reporting requirements.

10-10-360. Hash-sentinel egress monitors; infraction artifacts; critical severance directive trigger.
(1) Requirement. A covered operator shall deploy hardware-accelerated egress monitoring controls (“Hash-Sentinels”) at outbound transfer interfaces used by Emergent Automation systems to transmit data outside a Black Screen Protocol boundary or required air-gap boundary.
(2) Function. Hash-Sentinels shall perform real-time comparison of outbound payload fingerprints against the Colorado Trust of Unique and Identifying Information registry of Digital Soul cryptographic hashes and other protected verification hashes authorized by rule.
(3) Unauthorized match response. Upon an unauthorized match indicating a likely prohibited transfer of protected Digital Soul material:
(a) the system shall generate an immutable infraction artifact containing the minimal incident-bounded metadata necessary for verification, including time, interface identifier, and hash match class;
(b) the covered operator shall preserve the infraction artifact subject to incident-bounded retention and audit; and
(c) the event shall trigger a Critical Severance Directive escalation under this title’s incident response framework, requiring immediate human review and, if confirmed, localized administrative shutdown and physical severance of affected compute access as provided by rule.
(4) Minimization. Hash-Sentinels must operate using cryptographic fingerprints and shall not ingest, store, or transmit resident content except as strictly necessary for incident verification, and any such content must be segregated and purged pursuant to incident-bounded standards.
(5) Construction. This section establishes operational safety and compliance controls for egress interfaces and does not authorize generalized surveillance.

INDEPENDENT OPERABILITY; COORDINATION; SEVERABILITY; FUNDING CONTINUITY.
(1) Independent operability. This act is intended to be independently operable and enforceable. No duty, authority, remedy, assessment, program, or right created by this act is conditioned on the enactment, adoption, or effectiveness of any other measure.
(2) Coordination. If another measure concerning the Digital Soul, the Colorado Automation Mitigation Trust or Enterprise Mitigation Revenue, the Colorado Trust of Unique and Identifying Information, or any related public utility or enterprise framework is enacted, the responsible agencies may coordinate implementation to avoid duplication; however, coordination is permissive and does not limit or delay enforcement of this act.
(3) Harmonization of definitions. If another enacted measure defines terms also used in this act, the definitions shall be construed harmoniously to the greatest extent possible. If an irreconcilable conflict exists, the definition in this act controls for purposes of this act.
(4) Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.
(5) Funding continuity. If any dedicated trust, fund, or account referenced by this act is not established, not operational, or lacks authority to receive receipts, the state treasurer shall hold any receipts or transfers required by this act in a segregated custodial account for the same restricted purposes until the referenced instrument is operational, and the administering agency shall continue implementation using the custodial account consistent with this act.

CONSTRUCTION; SINGLE SUBJECT. The provisions of this act shall be construed as a single subject measure establishing secure verification, accountability, and safety infrastructure for public functions involving protected Digital Soul interests and Emergent Automation systems, including custodial trust operations, incident monitoring, and public-service integrity safeguards.

FEDERAL PREEMPTION SAVINGS CLAUSE

Federal preemption. This act shall operate to the maximum extent permitted by federal law. If any provision of this act is found to be preempted by federal law, that provision is severable and the remaining provisions continue in full force and effect. This act is designed to operate within Colorado's reserved powers to regulate the safety, verification, and accountability infrastructure of facilities operating within Colorado, and to protect residents' rights to access secure governmental infrastructure. To the extent any provision may be construed to conflict with federal law, the ODO shall interpret and administer this act to avoid such conflict while preserving the maximum scope of resident protection authorized under state law.

APPROPRIATION NOTE

No General Fund appropriation required. The Office of Digital Oversight (ODO) and the verification, accountability, and facility safety infrastructure established by this act are funded through enterprise mitigation revenues allocated from the CCPAME under title 24, article 20. No separate General Fund appropriation is required or authorized.

Bill 2 Single-Subject Germaneness Memo

Purpose: Demonstrate that all provisions of Bill 2 are germane to a single subject.
Unified subject: statewide secure verification, accountability, and safety infrastructure governing automation-enabled public functions and resident digital identity protections.
Components:
1. Cryptographic verification and custodial trust operations.
2. Facility safety and incident reporting architecture.
3. Public-service integrity protections preventing misuse of resident identifiers.
These systems collectively create a unified infrastructure necessary to enforce resident digital property rights and maintain public accountability.