DRAFT LEGISLATION

Verifiable Identity and Digital Autonomy Act

VIDA

FOR the purpose of mandating the design and implementation of privacy-preserving, citizen-controlled, decentralized digital identity systems; establishing fiduciary duties for government handling of personal data; ensuring equitable access to digital public services while maintaining and enhancing individuals' personal digital autonomy; prohibiting surveillance and centralized data dependencies; incorporating Fair Information Practice Principles; providing enforcement mechanisms and citizen rights; and generally relating to digital identity and government services. *Companion statute to the Personal Data Trusteeship Act (PDTA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA)*

Prepared by Michael G. Leahy

Initial Draft | March 2026

Be it enacted by the [Legislative Body] as follows:

Section 1. Short Title

(a) This Act shall be known as the Verifiable Identity and Digital Autonomy Act, or the "VIDA Act" or "VIDA."

Section 2. Legislative Findings and Purpose

(a) Findings

The Legislature finds that:

(1) Digital transformation offers significant opportunities to improve the accessibility, efficiency, and quality of government services, while posing serious risks to individual privacy, data security, autonomy, civil liberties, and public trust in the absence of enforceable constitutional constraints on how government designs and operates its digital infrastructure;

(2) Public trust in government is declining due to opaque data practices, centralization of personal information, surveillance-capable systems, and the absence of enforceable fiduciary obligations on government data handlers;

(3) Current digital identity and service delivery models fail to replicate the privacy-respecting, minimal-disclosure norms of the analog world, where a citizen who presented a paper credential to a government official disclosed only what was on the credential and retained everything else in their own possession;

(4) Applying fiduciary duties to the government's use of personal data establishes an essential foundation for trust, transparency, and individual empowerment, consistent with the scholarly framework establishing government as a constitutional trustee of citizen information;

(5) In the absence of enforceable standards, government and commercial actors may engage in rent-seeking behavior, including monopolization of digital identity infrastructure and unnecessary aggregation of personal data;

(6) Open, decentralized identity frameworks offer privacy-preserving alternatives to centralized systems and promote compliance with the Fair Information Practice Principles (FIPPs);

(7) Individual liberty, equitable access, and trustworthiness must be preserved by affirming the principles of data minimization, interoperability, transparency, and fiduciary duty in all government digital systems;

(8) The evolution of privacy rights in the digital era requires that individuals retain meaningful control over their personal data, including the ability to access, correct, delete, and transfer their information; and

(9) Modern integrated government databases possess all four characteristics that the Founders condemned as the hallmarks of general warrants: perpetual duration, universal scope, discretionary official access, and delegable authority, and are therefore constitutionally suspect regardless of the administrative convenience they provide.

(b) Purpose

The purpose of this Act is to:

(1) Maintain and enhance individuals' personal digital autonomy by empowering them with full control over their digital identities, credentials, and data across all interactions;

(2) Mandate the design and implementation of government digital services based on the principles of utility, security, and individual autonomy;

(3) Protect individual liberty by ensuring that digital identity systems operate without surveillance, remote verification dependencies, or undisclosed data transmissions to issuing authorities;

(4) Establish fiduciary duties of loyalty, care, confidentiality, and portability as binding obligations for all government handling of personal data;

(5) Require the deployment of verifiable, privacy-preserving, citizen-controlled, decentralized digital identity systems;

(6) Ensure that identity systems prevent third-party tracking, support cryptographically verifiable credentials, and maintain auditable and secure records of identifier states and transitions under user control;

(7) Incorporate Fair Information Practice Principles to minimize data collection, restrict use to narrowly defined purposes, and impose strict limitations on data retention;

(8) Prioritize technical designs that eliminate centralized dependencies while preserving privacy, interoperability, and long-term verifiability;

(9) Ensure equitable access to digital public services for all individuals regardless of background, disability, or digital literacy;

(10) Prevent rent-seeking behavior in the development and operation of digital identity infrastructure;

(11) Mandate fiduciary responsibilities for government actors and contractors managing personal data; and

(12) Affirm the right of individuals to exercise granular control over their personal data, including consent management, data access, correction, erasure, and portability.

(13) Establish a duty of ecosystem participation, distinct from the fiduciary duties this Act imposes on government, binding Commercial Participants that rely on the Verifiable Digital Identity Framework established by Section 7 without acting as government contractors.

(c) Legal Foundations

This Act is grounded in the following legal principles:

(1) Existing legal doctrines, including fiduciary duty, due process, and public trust, apply fully in digital contexts;

(2) Entities handling personal or identity-related data for public services are digital fiduciaries with enforceable duties under Section 4 of this Act; Commercial Participants that handle identity attributes through the Framework established by Section 7, without themselves performing a public service or acting under government contract, owe the distinct duty of ecosystem participation established by Section 4C;

(3) Individuals may challenge the legal authority of digital systems that affect rights without specific statutory authorization;

(4) Digital infrastructure must serve public purposes lawfully, equitably, and with minimal intrusion; and

(5) Due process must extend to automated systems, securing notice, explanation, and redress, as further developed in GAAFA.

(6) The state constitutional grounding established in PDTA Section 2(a)(9) through (12) applies with equal force to the digital identity architecture established by this Act.

Section 3. Definitions

In this Act, the following terms have the meanings indicated. Capitalized terms defined in PDTA or GAAFA have the same meanings as in those Acts unless this Act provides otherwise.

(1) ”Personal data” means any information relating to an identified or identifiable natural person;

(2) ”Fiduciary duty” means a legal and ethical obligation to act in the best interests of a data subject;

(3) ”Verifiable Credential” means a digitally signed assertion that can be cryptographically validated by any party without contacting the issuer, allowing the holder to selectively disclose specific information and control how the credential is presented;

(4) ”Self-Controlled Identifier” means a cryptographically derived identifier under the sole control of the individual, capable of supporting secure key rotation, recovery, delegation, and revocation, without requiring a centralized registry or continuous third-party oversight;

(5) ”Event Log Integrity” means the capacity of a system to maintain a tamper-evident, append-only record of key state transitions, including creation, rotation, and revocation, ensuring historical continuity and verifiability of identity control over time;

(6) ”Phone home” means any automatic or implicit communication from a verifier or credential presentation process to the original issuing authority or a third party, without the credential holder’s explicit consent at the time of verification;

(7) ”Surveillance” means any monitoring, tracking, logging, or analysis of identity verification events that is not strictly necessary for a user-directed transaction, consistent with PDTA Section 4A’s bilateral trust structure;

(8) ”Fair Information Practice Principles” or “FIPPs” refer to internationally recognized privacy principles including data minimization, purpose specification, use limitation, transparency, individual participation, and strict data retention controls;

(9) ”Verifiable State ID” means a digitally signed credential endorsed, or where necessary issued, by the state, held under the sole control of the individual in a secure personal digital wallet;

(10) ”Digital Wallet” means a secure, user-controlled software application capable of storing, presenting, and managing verifiable credentials without transmitting data to the issuing authority during presentation;

(11) ”Least Disclosure” means the principle that only the minimum data necessary for a specific, declared purpose is collected or shared;

(12) ”Digital Identity” means a set of electronically captured and verifiable attributes or credentials representing an individual’s identity;

(13) ”Decentralized Identifier” or “DID” means a globally unique, persistent, cryptographically verifiable identifier that does not require a centralized registration authority, consistent with standards published by the World Wide Web Consortium (W3C);

(14) ”Verifiable Credential” or “VC” means a cryptographically protected assertion made by an issuer about a subject, which can be presented and verified by third parties, consistent with W3C VC specifications;

(15) "Self-Sovereign Identity" or "SSI" means an identity system model that enables individuals to control and manage their identifiers, credentials, and personal data without reliance on a centralized intermediary;

(16) "Rent Seeking" means the pursuit of advantage through control over digital identity systems without proportional public value, including monopolization, barriers to autonomy, unnecessary data aggregation, or conduct inconsistent with fiduciary duties;

(17) "Open Standards" means publicly available technical specifications developed through a consensus process, freely usable and implementable without restriction, including the W3C VC and DID standards; and

(18) "Data Portability" means the right of individuals to obtain and reuse their personal data across different services and platforms, in a structured, commonly used, and machine-readable format.

(19) "Verifier" means a person or entity, other than a government agency or a government contractor subject to Section 4 of this Act, that receives, inspects, or evaluates a Verifiable Credential or Verifiable State ID presented by an individual for the purpose of confirming an identity attribute or eligibility fact;

(20) "Relying Party" means a person or entity, other than a government agency or a government contractor subject to Section 4 of this Act, that relies on a Verifier's confirmation, or on an individual's presentation of a Verifiable Credential or Verifiable State ID, to grant, deny, or condition access to a product, service, benefit, or transaction;

(21) "Digital Wallet Provider" means a person or entity, other than a government agency or a government contractor subject to Section 4 of this Act, that develops, operates, or provides a Digital Wallet used to store, present, or manage a Verifiable Credential or a Verifiable State ID;

(22) "Commercial Participant" means a Verifier, Relying Party, or Digital Wallet Provider, collectively;

(23) "Ecosystem Participation Agreement" means the agreement required by Section 4C(b) as a condition of certification under Section 7(b)(3).

Section 3A. Prohibition on Surveillance Architectures

Cross-references: PDTA Sec. 4A (Bilateral Trust Structure; secondary fiduciaries shall not repurpose data); PDTA Sec. 4A(c) (Prohibition on repurposing beyond original justified purpose); GAAFA Sec. 2(a)(4) (Opacity of government AI systems as constitutional threat)

The constitutional prohibition on general warrants, derived from the Fourth Amendment's guarantee against unreasonable searches and the historical condemnation of general search warrants by the Founders, applies to digital identity and data systems operated by government. Accordingly:

(a) Digital identity systems operated or funded by government shall not exhibit the characteristics of general warrants, including: perpetual duration of data access and retention

without time-limited authorization; universal scope of collection extending beyond the specific function for which data was collected; discretionary executive power to access, search, or correlate data without individualized justification; or delegable authority permitting broad classes of officials, contractors, and fusion partners to access personal data without specific, documented need.

(b) Centralized data aggregation enabling mosaic surveillance, meaning the use of government databases to generate comprehensive profiles of individuals from disparate data collected for different purposes, is prohibited as inconsistent with the Fourth Amendment's protections against unreasonable searches and the fiduciary framework established by PDTA.

(c) No government agency shall operate, fund, or contract for a digital identity or data system that, by its architecture, enables the continuous or retrospective monitoring of individuals' activities, associations, or movements, absent a specific judicial authorization for the specific individual and purpose.

Section 3B. Identity association as participatory act

Cross-references: VIDA Sec. 3A (Prohibition on Surveillance Architectures); VIDA Sec. 7(a)(13) (Rights of individuals to control digital identity); PDTA Sec. 4 (Establishment of Personal Data Trusteeship); PDTA Sec. 4A (Bilateral Trust Structure)

(a) Identity association, meaning the act of connecting a behavioral record, data profile, transaction history, or other information to a specific or identifiable natural person, is hereby recognized as an act requiring the individual's active participation. No government entity, and no entity acting on behalf of or in connection with a government function, shall associate behavioral data, location data, biometric data, or any other personal data with an identified or identifiable individual without that individual's active, informed credential presentation through the mechanisms established by Section 7 of this Act.

(b) Identity inference, meaning the use of technical attributes, behavioral patterns, probabilistic matching, or any other method to associate data with a specific or identifiable individual without that individual's active credential presentation, is prohibited for all government entities and entities acting in connection with government functions.

(c) For purposes of this section, "acting in connection with a government function" includes any entity that:

(1) Holds a contract, grant, or cooperative agreement with a government entity involving the handling of personal data;

(2) Provides data, analytics, algorithms, or profiling services purchased or licensed by a government entity; or

(3) Operates identity verification, authentication, or data matching systems on behalf of a government entity.

(d) The architectural standards established by Section 7 of this Act, including Decentralized Identifiers, Verifiable Credentials, selective disclosure, and zero-knowledge proofs, shall serve as the reference architecture for identity association in both government and commercial contexts. The [state agency] shall publish technical guidance enabling commercial entities to adopt these standards for identity association in private transactions.

Section 4. Data Fiduciary Duties

Cross-references: PDTA Sec. 6 (Obligations of Secondary Fiduciaries); PDTA Sec. 6A (Architectural Requirements for Fiduciary Compliance); GAAFA Sec. 4 (Constitutional and Fiduciary Foundations, extending these duties to AI deployment)

(a) Every government agency or contractor that collects, manages, or processes personal data in the provision of public digital services shall be deemed a data fiduciary with the following duties:

(1) Duty of Loyalty: To act in the best interests of the individual to whom the data pertains and not to use the data for purposes inconsistent with those interests, including sharing with law enforcement, commercial partners, or other government agencies beyond the original authorized purpose without fresh, explicit authorization;

(2) Duty of Care: To implement appropriate security, transparency, and governance practices to protect the integrity and confidentiality of personal data, including the Zero Trust Architecture required by Section 7(a)(5) and the data minimization requirements of Section 8;

(3) Duty of Confidentiality: To refrain from unauthorized disclosure, sale, or secondary use of personal data; and

(4) Duty of Portability: To enable individuals to access, download, and transfer their personal data and digital credentials to another provider or platform of their choice, in a structured, commonly used, and machine-readable format, without undue hindrance or delay.

(b) Enforcement and Accountability

(1) Any violation of the fiduciary duties or Fair Information Practice Principles established under this Act that results in demonstrable harm to an individual may be enforced through a private right of action. Agencies shall have a defense if they can demonstrate good-faith efforts to comply, including adherence to certified open standards under Section 6. The good-faith defense is not available to agencies that have failed to complete the required ADAs or AIAs under GAAFA;

(2) In any adjudicated proceeding in which a violation of the fiduciary duties of this Act is found, the agency or contractor in violation shall be liable for:

(i) Actual damages;

(ii) Statutory penalties as provided under this Act and PDTA Section 9;

(iii) Reasonable attorneys' fees and court costs; and

(iv) Any injunctive or equitable relief necessary to prevent ongoing or future violations;

(3) All penalties, fines, fees, and court-ordered payments associated with a final judgment under this Act shall be paid exclusively from the appropriated funds of the operating budget of the agency found to be in violation, and not from the general fund; and

(4) No officer or employee of a government agency shall be indemnified using public funds for damages arising from willful or knowing violations of the fiduciary duties of this Act. Indemnification may be available for negligent violations if the agency provided training and resources for compliance.

(c) Incentives for Compliance

(1) The government shall establish a grant program, funded through appropriations, to assist agencies in adopting compliant decentralized systems, including costs for audits, training, technology upgrades, and GAAFA compliance under GAAFA Section 13(f); and

(2) Agencies demonstrating full compliance through independent audits may receive priority in government funding allocations for digital initiatives.

(d) Consent and Transactional Procedures

All digital interactions between individuals and government agencies for the provision of public services, including the issuance of licenses, permits, benefits, or credentials, shall adhere to the following standardized, privacy-preserving process:

(1) Service Request Initiation: The portal shall provide detailed information about the service, including legal prerequisites, costs, and eligibility criteria, and confirm that the provided information matches the individual's request;

(2) Permission for Credential Query: The portal shall request explicit permission to query the individual's digital credentials to verify eligibility using privacy-preserving methods, including selective disclosure and zero-knowledge proofs, consistent with W3C standards for VCs and DIDs;

(3) Eligibility Assessment and Guidance: If permission is granted, the portal shall evaluate the queried credentials and, if criteria are not met, inform the individual of specific deficiencies and provide instructions on how to obtain or update necessary credentials;

(4) Confirmation of Eligibility and Intent: If criteria are met, the portal shall notify the individual of their eligibility and confirm their intent to proceed;

(5) Agency Commitments and Contractual Promises: Upon affirmative response, the portal shall present binding commitments from the agency, constituting an enforceable contractual agreement, including:

(i) Data Minimization: Collect only the minimum data required by law for the specific purpose;

(ii) Data Sequestration and Non-Disclosure: Store data in a purpose-specific database, not shared or accessed without explicit consent, consistent with PDTA Section 6A(a); and

(iii) Enforceable Rights for Breaches: Any breach grants a private right of action with statutory damages of $1,000 per instance and $100 per day the breach continues, plus actual damages, attorneys' fees, and injunctive relief;

(6) Individual Acknowledgment: The portal shall prompt the individual to confirm understanding and acceptance of these commitments;

(7) Data Collection Consent: The portal shall specify the exact data required and request formal consent for its collection; and

(8) Service Issuance: Upon consent, the agency shall issue the service as a digital verifiable credential, compliant with W3C standards, storable in the individual's digital wallet and not in a government database.

All steps shall be logged in a privacy-preserving, auditable manner consistent with PDTA Section 6A(c)'s immutable audit trail requirement. The government department responsible for information technology shall develop standardized templates and protocols for this process, ensuring consistency, accessibility, compliance with open standards, multilingual support, and accessibility guidelines.

Section 4A. Protections Against AI-Enabled Threats

Cross-references: PDTA Sec. 6A(d) (Cryptographic signatures for authentication); GAAFA Sec. 7 (Tiered AI Use Requirements); GAAFA Sec. 8 (Agentic AI as Statutory Secondary Fiduciary)

(a) Systems operating under this Act shall incorporate zero-knowledge proofs and cryptographic signatures to verify credentials without relying on detectable media. AI-generated synthetic media, including deepfakes and voice clones, shall be rendered legally irrelevant for identity verification purposes; only cryptographically signed credentials from the holder's digital wallet shall constitute valid verification. This requirement is consistent with PDTA Section 6A(d).

(b) Government shall not use AI or automated systems for surveillance or profiling of individuals without: a specific, individual probable cause finding for the specific person to be surveilled; judicial authorization consistent with the warrant requirements of the Fourth Amendment; and a defined, time-limited scope that does not permit generalized data collection beyond the specific authorized purpose. This prohibition applies to AI-powered facial recognition, predictive policing systems, social media monitoring, and any other AI application that enables continuous or retrospective profiling of individuals' activities, associations, or movements.

(c) Post-enactment regulations promulgated under Section 11 of this Act shall address emerging AI applications in government digital identity and data systems, ensuring that all such applications comply with the fiduciary duties of this Act and the specific requirements of GAAFA. No emerging AI application that was not specifically authorized at the time of

enactment may be deployed in a rights-affecting context without a finding by the Data Fiduciary Oversight Office that it is consistent with the constitutional principles underlying this Act, PDTA, and GAAFA.

Section 4B. Digital likeness and synthetic identity protections

Cross-references: VIDA Sec. 4A (Protections Against AI-Enabled Threats); GAAFA Sec. 4 (Constitutional and Fiduciary Foundations); CSDLPA Sec. 5 (Digital likeness protections)

(a) Definitions. For purposes of this section:

(1) "Digital likeness" means any compiled data profile, behavioral model, algorithmic representation, or other digitally constructed depiction of a specific or identifiable natural person, whether rendered in data, pixels, audio, or any other medium, that functions as a commercially or administratively operative representation of that person.

(2) "Compiled behavioral profile" means a record assembled from two or more data points about a specific or identifiable natural person's activities, transactions, movements, communications, associations, or other behavioral output, organized for the purpose of characterizing, predicting, scoring, classifying, or targeting that person.

(b) No government entity shall construct, maintain, purchase, license, or otherwise acquire a digital likeness or compiled behavioral profile of any individual except:

(1) Pursuant to a valid warrant supported by probable cause and satisfying the particularity requirement of the Fourth Amendment, specifically identifying the individual and the data elements to be obtained; or

(2) Through the individual's active, informed credential presentation under the mechanisms established by Section 7 of this Act, limited to the specific purpose for which the credential was presented.

(c) The prohibition in subsection (b) applies regardless of whether the digital likeness or compiled behavioral profile was originally assembled by a government entity, a commercial entity, or any other party. Government acquisition of commercially compiled profiles is subject to the same constitutional requirements as direct government compilation.

(d) A government entity's purchase, license, or receipt of commercially compiled behavioral data, location data, biometric data, or browser tracking data from a data broker, advertising network, or any other commercial source constitutes an acquisition subject to Fourth Amendment protections. The commercial origin of the data does not diminish, waive, or modify the constitutional requirements applicable to government acquisition.

Section 4C. Commercial Duty of Ecosystem Participation

Cross-references: VIDA Sec. 3 (Definitions: Verifier, Relying Party, Digital Wallet Provider, Commercial Participant, Ecosystem Participation Agreement); VIDA Sec. 4 (Data Fiduciary Duties, government and contractor track); VIDA Sec. 7(a)(2) (Purpose-limited use and zero-knowledge verification preference); VIDA Sec. 7(b)(3) (Certification of digital wallet providers and infrastructure operators); VIDA Sec. 10(e) (Private Right of Action); PDTA Sec. 4B(d) (Purely commercial data collection outside government connection governed by CSDLPA)

(a) Nature of the Duty. A Commercial Participant owes a duty of ecosystem participation to each individual whose identity attributes it processes through the Framework established by Section 7 of this Act. This duty arises from the Commercial Participant's acceptance of an Ecosystem Participation Agreement as a condition of certification under Section 7(b)(3), not from the constitutional relationship that grounds Section 4. The duty is contractual and, subject to subsection (c), may be satisfied through the individual's consent.

(b) Conditions of Participation. No person or entity may act as a Verifier, Relying Party, or Digital Wallet Provider within the Framework established by Section 7 unless it has executed an Ecosystem Participation Agreement with [the government department responsible for information technology] requiring the Commercial Participant to:

(1) use identity attributes obtained through the Framework only for the purpose stated to the individual at the time of the transaction;

(2) collect or request only the minimum identity attributes necessary for the stated transaction; where verification of a discrete fact would suffice, credential-based verification through the cryptographic methods required by Section 7(a)(2) is the required default. Collection of the underlying identity attribute instead requires an affirmative, documented determination, made and recorded before collection, that credential-based verification was not technologically feasible for the specific transaction. The determination shall be retained and made available to the individual or to [the government department responsible for information technology] upon request;

(3) not retain identity attributes obtained through the Framework beyond the period reasonably necessary for the stated purpose;

(4) not sell, license, rent, transfer, or otherwise monetize identity attributes obtained through the Framework, except pursuant to authorization meeting the requirements of subsection (c);

(5) not use identity attributes obtained through the Framework to build, augment, or contribute to a profile of the individual beyond what the stated transaction purpose requires;

(6) not link or correlate identity attributes or records of a presentation with identity attributes or behavioral data collected in an unrelated presentation or context;

(7) maintain technical and administrative safeguards commensurate with the sensitivity of the identity attributes held; and

(8) provide the individual a functioning, no-penalty mechanism to revoke any authorization previously granted under this section, effective within [72 hours] of revocation.

(c) Authorization Standard. A Commercial Participant satisfies subsections (b)(1) and (b)(4) with respect to a use, sale, or transfer otherwise prohibited by this section only if the individual's authorization:

(1) is specific to the particular use, sale, or transfer, and not stated in general or categorical terms;

(2) is not obtained through a dark pattern, deceptive interface, or bundled or pre-selected consent mechanism;

(3) is not made a condition of the individual's access to an unrelated product, service, or benefit; and

(4) is revocable at any time without penalty, consistent with subsection (b)(8).

(d) Non-Substitution. Nothing in this section diminishes, substitutes for, or is a defense to the duties established by Section 4. A government agency or contractor may not rely on a Commercial Participant's compliance with this section, or on an individual's consent given to a Commercial Participant under this section, to satisfy its own obligations under Section 4. Consent given under this section binds only the Commercial Participant that obtained it.

(e) Presumptively Disloyal Practices. A practice described in this subsection is a presumptive violation of the duty established by this section:

(1) transferring, selling, licensing, or otherwise disclosing identity attributes obtained through the Framework to a data broker, data aggregator, or other third party whose business consists primarily of compiling or reselling personal information, without authorization meeting the requirements of subsection (c);

(2) using identity attributes obtained through the Framework for a purpose other than the purpose stated to the individual at the time of the transaction, without authorization meeting the requirements of subsection (c);

(3) collecting an underlying identity attribute without the affirmative, documented, pre-collection determination required by subsection (b)(2); and

(4) any failure to comply with subsections (b)(5) through (b)(8).

(f) Rebuttal. The presumption established by subsection (e) is rebutted:

(1) for paragraph (e)(3), by production of the affirmative, documented, pre-collection determination required by subsection (b)(2); and

(2) for all other paragraphs of subsection (e), by a preponderance of the evidence that the practice was authorized in a manner meeting the requirements of subsection (c), or that the practice was required by law.

(g) Enforcement. An individual whose identity attributes are processed by a Commercial Participant is a third-party beneficiary of that Commercial Participant's Ecosystem Participation Agreement and may enforce its terms, including the requirements of subsections (b) and (e), through the private right of action established by Section 10(e) of this Act. The

[government department responsible for information technology] may suspend or revoke a Commercial Participant's certification under Section 7(b)(3) for material or repeated violations of this section.

Section 5. Implementation and Transition

Cross-references: VIDA Sec. 11 (Implementation and Timelines); GAAFA Sec. 13 (Implementation and Timelines, coordinated with this Act)

(a) Within [one year] of enactment, the [state agency] shall develop a phased plan to migrate from legacy centralized systems to decentralized frameworks compliant with this Act, prioritizing high-risk areas including vital records, benefits eligibility, licensing, and any system identified as posing elevated risk to individual liberty under the fiduciary framework of PDTA.

(b) Pilot programs shall test interoperability with existing systems, with public input collected through the public comment process required by Section 9 of this Act. Pilot results shall be published publicly before any large-scale deployment.

(c) Training and support shall be provided to government personnel and citizens to ensure equitable access to compliant digital identity systems, including offline alternatives for non-digital users consistent with Section 12 of this Act.

Section 6. Open Digital Identity Standards

Cross-references: PDTA Sec. 4(c) (Secondary fiduciaries must obtain explicit authorization); GAAFA Sec. 12 (Vendor Obligations and Procurement Standards, extending these requirements to AI Vendors)

(a) All government-managed or government-funded digital identity systems shall:

(1) Support Verifiable Credentials and Decentralized Identifiers based on open standards, including W3C VC and DID specifications;

(2) Allow for selective disclosure and data minimization, enabling citizens to prove specific facts without disclosing the underlying personal data that establishes them;

(3) Avoid mandatory use of a single private platform or centralized intermediary, consistent with the monopoly prevention requirements of Section 7(a)(15); and

(4) Provide mechanisms for user-directed export and transfer of identifiers, credentials, and personal data, supporting seamless switching between providers without loss of continuity.

(b) Any trust registry or verification infrastructure used in connection with government digital identity systems shall be publicly auditable, interoperable, and free from exclusive control. No private entity shall be permitted to control the only available trust registry for a government digital identity system.

Section 7. Verifiable Digital Identity Framework and Decentralized Identity Protections

Cross-references: PDTA Sec. 4A(b) (Government as limited secondary fiduciary; endorsement using cryptographic methods without data retention); GAAFA Sec. 5 (Algorithmic Deployment Assessment, referencing this section); GAAFA Sec. 7 (Tiered AI Use Requirements, referencing this section's minimization principles)

The government shall develop and maintain a Verifiable State ID system aligned with decentralized, open standards to enhance user autonomy, incorporating the following characteristics:

(a) Verifiable Digital Identity Framework Requirements.

(1) Holder Control: Individuals shall retain exclusive control over their credentials, including the ability to store, present, and revoke credentials via a personal digital wallet. No government agency shall access, monitor, or receive notification of credential presentations without the holder's explicit, per-transaction consent;

(2) Purpose-Limited Use: Identity verification or eligibility determination shall rely on cryptographic yes/no queries rather than raw data transmission as the required default, ensuring that verification of a fact does not require disclosure of the personal data underlying that fact. Raw data transmission is permitted only upon an affirmative, documented determination, made and recorded before the transmission, that cryptographic verification was not technologically feasible for the specific transaction, consistent with PDTA Section 6A(b)'s zero-knowledge verification preference and its documentation requirement, and recorded in the audit trail required by PDTA Section 6A(c);

(3) No Surveillance Capabilities: Credentials shall not enable or require server-based verification during presentation and shall support offline, holder-controlled, cryptographic verification mechanisms that preserve anonymity and unlinkability unless explicitly waived by the holder in the specific transaction. Phone home capabilities are prohibited;

(4) Delegation Support: The system shall support privacy-preserving identity presentation by minors, dependents, or legal proxies, consistent with the guardianship provisions of PDTA Section 5(c);

(5) Zero Trust Architecture Requirement: All identity verification and access control systems shall:

(i) Assume breach at every layer and continuously verify cryptographic authorization;

(ii) Prohibit shared secrets, including passwords and knowledge-based authentication;

(iii) Reject multi-factor authentication relying on device-bound secondary factors tied to centralized services;

(iv) Require cryptographic, decentralized, public key-based authentication tied to holder-controlled identity material; and

(v) Treat every identity assertion as independently verifiable without persistent state or prior relationship assumptions;

(6) Preference for Decentralized, Open Standards-Based Methodologies: The identity framework shall utilize methodologies that:

(i) Enable individuals to generate, control, and manage identifiers and credentials independently;

(ii) Employ cryptographically verifiable event logs or credential chains for secure key rotation, delegation, and recovery;

(iii) Support issuance and presentation of independently verifiable credentials;

(iv) Align with open standards for decentralized identity and verifiable credentials; and

(v) Facilitate selective disclosure and minimal data exposure;

(7) Credential Structure and Presentation: Digital credentials shall be tamper-evident, cryptographically verifiable, and selectively disclosable, with metadata specifying issuer, subject, expiration, and verification material. Credentials shall support chaining of authenticated data to ensure provenance and integrity across multiple assertions or events;

(8) Identifier Architecture: Digital identities shall be anchored in self-controlled identifiers supporting key rotation without reissuance, resolvable without centralized registries, and supporting delegation and recovery;

(9) Event Log Integrity and Key State Continuity: Systems shall implement append-only key state logs under holder control, ensuring verifiable continuity and provenance of key events through cryptographic commitments and receipts that allow for ambient verifiability without reliance on a single authority;

(10) Auditable Verification and Data Minimization: Credential verifiers shall perform full cryptographic validation without requiring online access, operate under data minimization principles, and allow holders to audit and control verification requests;

(11) Self-Sovereign Identity Alignment: The framework shall be compatible with decentralized identity systems supporting user-controlled identifiers and cryptographically verifiable credentials;

(12) Preference for Endorsement: The government shall prefer endorsement of digital credentials issued by accredited private or decentralized entities over direct government issuance, to minimize centralization, reduce government liability, promote interoperability, and encourage private innovation, consistent with PDTA Section 4A(b)'s authorization for government to endorse rather than create identity. Direct government issuance is permitted only where no suitable endorsed credential is available for a specific public function;

(13) Rights of Individuals to Control Digital Identity: Every resident shall have the right to create, use, manage, correct, delete, and transfer digital identifiers under their exclusive control, including decentralized identifiers. No government agency shall require use of a single, centralized identity provider as a condition of receiving public services unless required by law

and no secure and privacy-preserving alternative is reasonably available. The issuance and use of any digital credential by a public agency shall be limited to the specific purpose for which it was issued and subject to revocation, portability, and user-directed export;

(14) Interoperability, Portability, and Open Access Standards: Identity systems shall:

(i) Comply with open, public, and non-proprietary standards, including W3C VC and DID;

(ii) Support open-source protocols or similar decentralized trust mechanisms that do not rely on centralized key registries;

(iii) Permit user-managed export, portability, and revocation of identifiers and credentials;

(iv) Support selective disclosure, zero-knowledge proofs, or other cryptographic means to validate claims while minimizing disclosure of personal information; and

(v) Ensure all identity systems support data portability and interoperability, allowing users to seamlessly transfer data and credentials between compliant platforms, avoiding central data aggregation in favor of cryptographic proofs and decentralized verification models;

(15) Monopoly Prevention and Open Participation: No public agency shall:

(i) Enter into exclusive licensing agreements for identity infrastructure;

(ii) Require storage of data in a centralized repository beyond what is operationally necessary to meet the specific legal purpose for which the data is collected, with all personally identifiable data stored solely in a data structure associated only with that specific legal purpose and comprising the minimal data necessary to fulfill it; or

(iii) Deny participation to competing, standards-compliant providers on discriminatory terms. All identity systems funded with public dollars shall be made available on fair, reasonable, and non-discriminatory (FRAND) terms; and

(16) Governance and Auditability: Any registry or trust anchor used by a government agency shall:

(i) Be governed by a multi-stakeholder board including civil liberties and public interest groups;

(ii) Publish governance rules and receive public comment; and

(iii) Submit to independent security and governance audits on at least an annual basis, the results of which shall be made publicly available.

(b) Implementation and Rulemaking: The government department responsible for information technology shall promulgate regulations to:

(1) Define technical and legal requirements for compliant decentralized identity systems and certify decentralized identity systems and credentialing platforms for compliance with this section;

(2) Define and enforce data minimization, interoperability, and portability requirements;

(3) Certify digital wallet providers and infrastructure operators; and

(4) Establish procedures for equitable access to decentralized identity by underserved populations, including those without broadband access, banking services, or government-issued ID. All government agency procurements related to digital identity shall comply with this Act within 24 months, with extensions up to 12 months granted based on written justification.

Section 8. Data Minimization and Sequestered Databases

Cross-references: PDTA Sec. 6A(a) (Purpose-Limited Sequestration); PDTA Sec. 6A(b) (Zero-Knowledge Verification Preference); GAAFA Sec. 7(a) (Tier 1 AI Use Requirements referencing this section); GAAFA Sec. 8(b) (Agentic AI authorization requirements referencing this section)

(a) No government agency shall maintain centralized repositories of personal information beyond what is necessary for a declared, legally authorized purpose. The prohibition on general-purpose databases applies regardless of whether the database was assembled through intentional aggregation or the accumulated effect of individually authorized collections.

(b) Agencies shall architect systems to maintain sequestered, purpose-specific datasets, minimizing lateral access or correlation between datasets, with each data use independently auditable and subject to retention limits. Each dataset shall be accessible only to the agency functions for which it was specifically created, and cross-agency access shall require both fresh authorization from the data subject trustee and a documented legal basis.

(c) All government data infrastructure shall follow Zero Trust principles, prohibiting lateral access across datasets and requiring mutual authentication through cryptographic mechanisms, consistent with Section 7(a)(5). The Zero Trust requirement applies to AI systems and Agentic AI Systems that access government data, as specified in GAAFA Section 8(b)(4).

(d) A government data fiduciary shall collect only the minimum personal information necessary for a specific, legally authorized purpose, articulated at the time of collection. The purpose shall be specific enough that a person of reasonable intelligence can understand what data will be collected, why it is needed, and what will be done with it.

(e) All data collection, processing, and retention shall adhere to Fair Information Practice Principles, including:

(1) Collecting only the minimum data necessary;

(2) Collecting data for a single, clearly defined purpose;

(3) Prohibiting reuse or repurposing without explicit consent, consistent with PDTA Section 4A(c); and

(4) Securely deleting or anonymizing data upon fulfillment of purpose unless legally required otherwise.

(f) Where feasible, agencies shall confirm facts without collecting supporting data, using cryptographic queries or verifiable credentials, consistent with PDTA Section 6A(b)'s zero-knowledge verification preference.

(g) Centralized, multipurpose data lakes are prohibited. Personal data shall be stored in discrete, sequestered, purpose-specific datasets enforcing Zero Trust principles. Any data infrastructure that permits cross-purpose querying, aggregation, or profiling without individualized authorization for each cross-purpose access violates this section regardless of its technical architecture.

Section 9. Public Participation and Accessibility

Cross-references: GAAFA Sec. 9(d) (Public filing of Algorithmic Impact Assessments); GAAFA Sec. 10(a)(3) (Transparency registry)

(a) Digital identity systems shall be designed for equitable access by residents of all communities, including those with disabilities, limited internet access, or limited English proficiency. Universal design principles shall be applied to all government digital identity infrastructure.

(b) Agencies shall publish open data use impact assessments and receive public comment prior to adopting new identity or verification systems. Impact assessments shall be written in plain language, published for public comment at least [60] days before adoption, and shall specifically address privacy implications, surveillance risks, disparate impact on protected classes, and fiduciary compliance. For AI-enabled identity or verification systems, impact assessments shall satisfy the requirements of GAAFA Section 9.

Section 10. Citizen Rights and Enforcement Mechanisms

Cross-references: PDTA Sec. 5(b) (Rights of Data Subject Trustees); PDTA Sec. 8 (Private Rights of Action); GAAFA Sec. 6 (Right to Algorithmic Explanation); GAAFA Sec. 11 (Enforcement)

(a) Individual Rights

Every individual shall have the right to:

(1) Know what data the government holds about them, including a complete list of all data elements, the purpose for which each was collected, and the length of time it has been retained;

(2) Access, correct, or request deletion of personal data held by government, with government compliance within [30 days] of a verified request, consistent with PDTA Section 5(b)(3);

(3) Withhold consent for secondary uses beyond mandatory legal requirements and to be informed of the specific legal authority, if any, compelling any non-consensual data use;

(4) Use digital government services without forced disclosure beyond what is strictly required for the specific service and without surveillance of that use, consistent with PDTA Section 4A's bilateral trust structure; and

(5) Bring a civil action for damages, declaratory relief, and injunctive relief for violations of this Act, consistent with PDTA Section 8.

(b) Heightened Scrutiny

Courts shall afford heightened scrutiny to any government or commercial surveillance or remote verification practice not in compliance with this Act. The burden of justifying non-compliant practices rests on the government entity asserting the necessity of the practice, not on the individual challenging it.

(c) Data Fiduciary Oversight Office

The government shall establish a Data Fiduciary Oversight Office to:

(1) Investigate complaints and enforce fiduciary obligations under this Act and GAAFA;

(2) Publish transparency reports and audit summaries, including the annual AI deployment report required by GAAFA Section 10(a)(4);

(3) Impose penalties and remediation orders, including suspension of procurement eligibility and public disclosure of non-compliance; and

(4) Fulfill the AI-specific mandates assigned to the Oversight Office by GAAFA Section 10(a).

(d) Attorney General

The Attorney General shall have enforcement authority under this Act, consistent with PDTA Section 10 and GAAFA Section 11(e).

(e) Private Right of Action

A private right of action is available to any resident harmed by a knowing or reckless violation of this Act, with remedies including:

(1) Injunctive relief;

(2) Statutory or actual damages, consistent with PDTA Section 9;

(3) Attorneys' fees and court costs; and

(4) For violations of data portability, access, correction, or erasure rights: injunctive relief and statutory damages as specified in Section 4(d)(5)(iii).

Section 11. Implementation and Timelines

Cross-references: GAAFA Sec. 13 (coordinated implementation timelines)

(a) Within [7] months of enactment, the Chief Information Officer shall issue technical standards for:

(1) Verifiable credential issuance and validation, prioritizing decentralized methodologies;

(2) Offline-capable digital wallet interoperability;

(3) Secure, citizen-controlled data sharing protocols;

(4) A Zero Trust Architecture framework prohibiting shared secrets and specifying cryptographic identity mechanisms;

(5) Credential structure and presentation under Section 7(a)(7);

(6) Identifier architecture under Section 7(a)(8); and

(7) Event log integrity and key state continuity under Section 7(a)(9).

(b) New or re-platformed digital services shall comply within [24] months of this Act's effective date.

(c) Existing services shall be retrofitted within [48] months unless granted a waiver by the Oversight Office for good cause.

Section 12. Digital Equity and Inclusion Mandate

(a) The government shall ensure equitable access to digital services for all individuals, including minors, the elderly, individuals with disabilities, the unhoused, and those with limited digital access or limited English proficiency.

(b) Agencies shall:

(1) Provide non-digital alternatives where necessary, ensuring that no individual is denied access to government services solely because they cannot or choose not to use digital identity systems;

(2) Partner with community organizations for onboarding and support, particularly for populations historically underserved by digital government services; and

(3) Develop inclusive interfaces with multilingual and assistive capabilities, consistent with applicable accessibility standards and the equity mandate of PDTA Section 7(b)(2).

Section 13. Severability

(a) If any provision of this Act or its application to any person or circumstance is found invalid or unenforceable, the remaining provisions shall remain in full force and effect.

(b) A jurisdiction adopting this Act may enact Sections 1 through 4B and Sections 5 through 18 without enacting Section 4C. A jurisdiction that has enacted an equivalent government-facing digital identity framework by other means may enact Section 4C independently of the remainder of this Act. Enactment of Section 4C alone does not create or imply any fiduciary duty on the part of government under Section 4.

Section 14. Effective Date

(a) This Act shall take effect [180] days after enactment.

Section 15. Cross-Referencing and Statutory Construction

(a) This Act shall be construed in harmony with the Personal Data Trusteeship Act (PDTA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA) to create a comprehensive and integrated framework for constitutional digital governance. VIDA provides the technical architecture; PDTA provides the legal superstructure of fiduciary obligations; GAAFA governs the AI decision layer. Where this Act and PDTA or GAAFA address the same subject matter, the provision that provides greater protection to the individual's rights shall govern.

(b) This Act does not limit any right or remedy available to a citizen under PDTA, GAAFA, the Fourth Amendment to the United States Constitution, applicable civil rights statutes, or any other provision of law.

Section 16. Sunset Review

(a) The Data Fiduciary Oversight Office shall review this Act and report to [the Legislative Body] on its implementation, effectiveness, and recommended amendments every [5] years following the effective date. The review shall specifically assess whether the technical standards of Section 7 remain current with developments in decentralized identity technology, whether the monopoly prevention provisions of Section 7(a)(15) require strengthening, and whether the integration of this Act with PDTA and GAAFA requires updating.

Section 17. Funding and Resources

(a) The [state agency] shall allocate funds from [source] to support implementation of this Act, including:

(1) Technical standard development and the work of the Chief Information Officer under Section 11;

(2) Establishment and staffing of the Data Fiduciary Oversight Office under Section 10(c);

(3) The grant program for agencies adopting compliant decentralized systems under Section 4(c)(1);

(4) Public education campaigns and tool development for low-digital-literacy populations; and

(5) Coordination with PDTA implementation funding under PDTA Section 15 and GAAFA implementation funding under GAAFA Section 13(f) to avoid duplication and maximize efficiencies.

Section 18. Oversight and Reporting

(a) A Data Fiduciary Oversight Board, including citizen representatives, civil liberties advocates, and technical experts, shall monitor compliance under this Act and issue annual reports on the state of government digital identity infrastructure, identified risks, enforcement actions taken, and recommendations for improvement, consistent with the multi-stakeholder governance requirement of Section 7(a)(16).

(b) Individuals shall have access to personal data logs maintained pursuant to PDTA Section 6A(c), with automatic notifications for new data queries within [48 hours] of each query.

About this Draft

This is an initial formatted draft of the Verifiable Identity and Digital Autonomy Act (VIDA), prepared as a companion statute to the Personal Data Trusteeship Act (PDTA) and the Government Algorithmic Accountability and AI Fiduciary Act (GAAFA). All bracketed provisions indicate items requiring legislative specification. Cross-references to PDTA and GAAFA reflect the section numbering of the March 2026 drafts of those Acts. This draft is prepared for discussion and does not represent the position of any government body.