

VERIFIABLE IDENTITY AND DIGITAL AUTONOMY ACT

VIDA VERSION 2.2

Clean Restated Legislative Candidate

An Act to establish requirements for government digital identity, credential, verification, authentication, authorization, interoperability, and digital-service architecture; to preserve individual digital autonomy; to constrain governmental informational capability according to lawful governmental authority; to provide for privacy-preserving verification, selective disclosure, purpose sequestration, open standards, accessibility, portability, and vendor independence; to prohibit surveillance-capable identity infrastructure and Government Population Golden Records; to establish requirements for commercial participation in government-recognized identity ecosystems; and generally to implement the Personal Data Trusteeship Act and the Fiduciary Commons Government Information Architecture Standard in digital identity and public-service infrastructure.

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

SECTION 1. SHORT TITLE

This Act may be cited as the “Verifiable Identity and Digital Autonomy Act,” “VIDA Act,” or “VIDA.”

SECTION 2. LEGISLATIVE FINDINGS, PURPOSE, AND GOVERNING ARCHITECTURE

(a) Findings

- (1) digital identity and digital public services can materially improve the accessibility, efficiency, reliability, security, and quality of governmental services;
- (2) the architecture through which government identifies, authenticates, verifies, authorizes, correlates, and serves persons determines not merely how information is processed but what informational capability government possesses;
- (3) traditional physical credentials frequently permit a person to establish an identity attribute or entitlement without automatically informing the issuer where, when, why, or to whom the credential was presented;
- (4) the architecture of digital systems should preserve or improve upon that informational restraint rather than transform ordinary identification into continuous governmental or commercial observation;
- (5) authentication of a person does not itself establish governmental authority to obtain all information concerning that person;
- (6) possession of an Identifier does not itself authorize cross-purpose correlation;
- (7) technical interoperability does not itself aggregate the governmental authority of participating agencies, governments, issuers, Verifiers, or Relying Parties;
- (8) government frequently needs an answer to a defined question rather than possession of all information from which the answer can be derived;

- (9)** privacy-preserving Credentials, Selective Disclosure, cryptographic proofs, purpose-specific Identifiers, offline Verification, Holder-Controlled Credential Environments, and other privacy-enhancing technologies can materially reduce unnecessary governmental and commercial knowledge;
- (10)** no single technology, topology, protocol, Credential format, or identity model is sufficient by itself to protect liberty;
- (11)** a nominally decentralized system may nevertheless create generalized informational power through federated search, common Identifiers, metadata, application programming interfaces, Identity Resolution, artificial intelligence, or other functional integration;
- (12)** a shared or centralized technical component may be consistent with this Act where its standing capability remains bounded to legitimate governmental authority and does not enable generalized individualized knowledge;
- (13)** digital identity architecture should therefore be evaluated by the governmental informational capability it creates rather than by topology alone;
- (14)** open standards, portability, interoperability, vendor independence, transparent trust infrastructure, and meaningful competition reduce rent seeking and institutional dependence;
- (15)** digital government must remain accessible to persons who cannot or choose not to use smartphones, commercial Wallets, biometrics, broadband connectivity, or other particular technologies;
- (16)** fiduciary duties, informational-authority principles, rights, architectural constraints, and remedies established by PDTA apply to governmental identity infrastructure;
- (17)** artificial intelligence and automated systems operating upon identity infrastructure possess no governmental authority independent of the governmental actors and functions they serve;
- (18)** modern digital systems can create functional equivalents of population-scale integrated dossiers even without a single centralized database;
- (19)** history underlying constitutional prohibitions against general warrants provides an important warning against governmental architectures creating perpetual, universal, discretionary, and broadly delegable informational power, although the statutory protections established by this Act do not depend upon a court first determining that a particular architecture constitutes a search under the Fourth Amendment; and
- (20)** government digital identity infrastructure should make it easy for government to establish facts it is legitimately authorized to establish while making it difficult or impossible through ordinary standing access to obtain materially more information.
 - (21)** Positive Legal Authority is a necessary source of governmental power but does not, by itself, establish that every technically available identity capability is legitimate or necessary as ordinary standing capability;
 - (22)** in voluntary citizen-originated identity and service transactions, the individual's specific purpose presumptively establishes the originating informational boundary, subject to independently sufficient law and the substantive informational-justification requirements of PDTA; and
 - (23)** legitimate authority establishes an outer ceiling on governmental informational power, not a procurement or system-design specification for the maximum capability government should maintain at all times.

(b) Purpose

- (1)** preserve and enhance individual Digital Autonomy;
- (2)** implement PDTA requirements of Ordered Informational Authority within government identity and digital-service infrastructure;
- (3)** cause Standing Technical Informational Capability to correspond to, and not materially exceed, Necessary Standing Informational Capability, which in turn SHALL remain within Standing Legitimate Informational Authority;
- (4)** distinguish Identification, Authentication, Technical Authorization, Attribute Verification, Identity Resolution, Credential Issuance, Credential Presentation, and Eligibility Determination as separate informational operations;
- (5)** promote Verification without unnecessary collection;
- (6)** prevent ordinary Credential use from becoming a mechanism for tracking individuals;
- (7)** prohibit Government Population Golden Records and Functional Universal Search through identity infrastructure;
- (8)** preserve Purpose Sequestration while permitting authorized interoperability;
- (9)** support Holder-Controlled Credential Environments, Authorized Information Trustees, guardianship, delegation, secure recovery, and portability;
- (10)** ensure accessibility and nondigital equivalence;
- (11)** promote open and interoperable technical standards without legislatively mandating a particular protocol or commercial technology;
- (12)** prevent vendor lock-in, informational rent seeking, and capability laundering;
- (13)** establish conditions governing participation by private entities in Government-Recognized Identity Ecosystems;
- (14)** integrate identity architecture with PDTA and GAAFA without duplicating their substantive regimes; and
- (15)** establish enforceable architectural requirements capable of evolving as technology changes.

(c) Governing Architectural Principle

A Government Agency SHALL design, procure, operate, and govern digital identity and digital-service infrastructure so that government may establish identity, attributes, eligibility, authority, or other facts necessary to a legitimate governmental function while minimizing the informational capability created by the interaction and without converting identity infrastructure into generalized governmental capability to know, correlate, track, or profile persons across purposes.

SECTION 3. DEFINITIONS

(a-1) PDTA Definition Inheritance

Capitalized terms defined by PDTA have the meanings established by PDTA unless this Act expressly defines a specialized identity or digital-service term. A specialized definition does not create Governmental Informational Authority by implication.

(a) Specialized Identity and Digital-Service Definitions

The following specialized definitions apply to identity and digital-service functions. They supplement PDTA and do not create Governmental Informational Authority by implication.

- (1) "Authentication"** means an informational operation establishing with an appropriate degree of assurance that an actor controls or is legitimately associated with an asserted Identifier, Credential, authenticator, device, key, account, or identity.
- (2) "Technical Authorization"** means the system-level determination that an authenticated or otherwise recognized actor may perform a defined operation upon a defined resource, information domain, service, or governmental function. Authentication does not itself constitute Technical Authorization, and Technical Authorization does not create Governmental Informational Authority or Materially Renewed Authorization.
- (3) "Attribute Verification"** means establishing whether a defined proposition concerning a person, organization, object, status, authority, eligibility, or relationship is true without necessarily obtaining the underlying information from which the proposition is derived.
- (4) "Certification"** means a formal determination under Section 23 that a person or service satisfies the requirements for participation in a Government-Recognized Identity Ecosystem. Certification does not constitute endorsement of the participant for activity outside the ecosystem.
- (5) "Commercial Participant"** means a nongovernmental person that participates in, seeks Certification for, or holds Certification to act as a Verifier, Relying Party, Credential Wallet Provider, or other private participant within a Government-Recognized Identity Ecosystem and is not acting as a Governmental Actor for the transaction at issue.
- (6) "Credential"** means a physical or digital assertion, record, document, cryptographic object, token, or other representation issued or endorsed by an authoritative source and capable of supporting Verification of one or more claims.
- (7) "Credential Presentation"** means an act through which a Credential, claim, proof, or derived assertion is presented or made available for Verification.
- (8) "Credential Surveillance Infrastructure"** means a system, feature, service, protocol, or capability designed or materially capable through ordinary operation of enabling cross-context monitoring, correlation, or reconstruction of Credential Presentations in a manner not necessary to the authorized transaction.
- (9) "Credential Wallet or Wallet"** means a technical environment used to hold, manage, present, delegate, recover, or otherwise exercise control over Credentials or associated cryptographic material.
- (10) "Credential Wallet Provider"** means an entity providing a Credential Wallet to individuals or Authorized Information Trustees.
- (11) "Digital Autonomy"** means the ability of a person, to the maximum extent consistent with lawful governmental authority, to control the custody, presentation, disclosure, portability, delegation, and Verification of Credentials and identity attributes without unnecessary governmental or commercial observation, correlation, or interference.
- (12) "Digital Identity"** means electronically represented Identifiers, Credentials, attributes, authenticators, relationships, authorities, or other information used to identify, authenticate, verify, authorize, or distinguish a person or entity.
- (13) "Eligibility Determination"** means application of substantive legal or program criteria to verified or otherwise lawfully obtained facts to determine whether a person qualifies for a governmental service, status, license, benefit, permission, obligation, or other governmental consequence.

(14) "Event Integrity" means the ability to establish the authenticity, sequence, and integrity of material Credential or Identifier lifecycle events, including issuance, activation, rotation, suspension, revocation, delegation, recovery, and expiration.

(15) "Government-Recognized Identity Ecosystem" means an identity or Credential framework in which the State establishes or recognizes technical, Certification, trust, interoperability, or participation requirements for nongovernmental participants.

(16) "Holder-Controlled Credential Environment" means an arrangement in which a person or the person's Authorized Information Trustee can exercise meaningful control over Credential custody, presentation, disclosure, delegation, portability, and recovery without unnecessary issuer or intermediary control.

(17) "Identification" means an informational operation determining or establishing which person, organization, device, object, or other entity is involved in a transaction or governmental function.

(18) "Identifier" means information, a number, name, cryptographic value, account reference, token, address, or other representation used to distinguish or reference an entity.

(19) "Identity Resolution" means an informational operation determining that two or more Identifiers, records, Credentials, accounts, events, or other informational artifacts concern or are associated with the same person or entity.

(20) "Minimum Knowledge Exposure" means limiting information revealed in a transaction to the minimum individualized or relational knowledge reasonably necessary for the authorized governmental purpose.

(21) "No-Phone-Home Verification" means Credential or Attribute Verification that does not require or cause an issuer or unrelated intermediary to learn of the presentation or Verification transaction except where such communication is independently necessary and authorized.

(22) "Open Standard" means a publicly documented technical specification available for implementation on fair, reasonable, and nondiscriminatory terms and not structured to create unnecessary proprietary dependence.

(23) "Pairwise Identifier" means an Identifier designed for use within a defined relationship or context so that ordinary use does not itself permit correlation across unrelated relationships or contexts.

(24) "Relying Party" means an entity that relies upon an identity assertion, Credential, Attribute Verification, Authentication, or other proof to make a decision or complete a transaction.

(25) "Selective Disclosure" means revealing only selected claims, attributes, proofs, or propositions rather than all information contained within or associated with a Credential.

(26) "Verifier" means an entity or system that evaluates a Credential, proof, claim, Authentication, Attribute Verification, or other identity assertion.

(27) "Verification" means the process of determining the authenticity, validity, status, integrity, provenance, or truth of a Credential, claim, attribute, assertion, or proof.

SECTION 4. RELATIONSHIP TO PDTA, GAAFA, AND FCGIAS

(a) Functional Allocation

PDTA governs the legal relationship, fiduciary duties, Governmental Informational Authority, individual rights, structural limitations, burdens, remedies, and enforcement applicable to

governmental information. This Act governs identity, Credential, Authentication, Technical Authorization, Verification, interoperability, and digital-service architecture. GAAFA governs artificial intelligence, algorithmic processing, automated decisions, derived computational outputs, and agentic systems.

(b) FCGIAS

FCGIAS provides FCGIAS Version 2.2 Candidate Standard as the current technical and conformance reference, only to the extent lawfully incorporated under PDTA for implementation of this Act as provided by PDTA.

(c) No Creation of Authority

Compliance with this Act establishes conditions governing the exercise of Governmental Informational Authority. Nothing in this Act independently creates authority to collect, identify, resolve, correlate, infer, disclose, retain, or act upon information.

(d) Harmonization

This Act shall be construed consistently with PDTA and GAAFA where reasonably possible. A specific statutory provision governing a particular identity operation controls over a more general implementation provision, subject to applicable constitutional law. A later enactment shall not be construed by implication to diminish protections established by this Act where the statutes can reasonably be harmonized.

(e) Common Trilogy Machinery

The PDTA provisions governing Composite Governmental Information Transactions, Responsible Government Agencies, Role Stacking, Exception Envelopes, the Trilogy Conformance Code, Vendor responsibility, burdens, remedies, and transition apply to identity and digital-service functions governed by this Act except where this Act expressly supplies a more specific rule.

SECTION 5. DIGITAL AUTONOMY

(a) General Rule

A person interacting with government retains Digital Autonomy except to the extent an independently sufficient governmental authority lawfully requires otherwise.

A person interacting with government retains Digital Autonomy except to the extent an independently sufficient governmental authority lawfully requires otherwise.

(b) No Mandatory Surrender of Unnecessary Information

Government SHALL NOT condition access to a governmental function upon disclosure of information unnecessary to that function.

(c) Credential Choice

Where multiple conforming Credential forms or presentation methods are reasonably available, government shall permit the person to select among them unless a documented legal, security, accessibility, or operational requirement reasonably requires a different method.

(d) No Mandatory Commercial Intermediary

Government SHALL NOT require a person to establish an account with, purchase services from, or surrender additional information to a private commercial identity provider as the exclusive means

of exercising a legal right or accessing a governmental service, except where specifically authorized by law and reasonably necessary.

(e) Delegation

Digital Autonomy includes the ability to exercise lawful delegation through an Authorized Information Trustee consistent with PDTA.

(f) No Consent Fiction

(g) Citizen-Originated Purpose

Where a person voluntarily initiates Credential issuance, Credential Presentation, Verification, or access to a nonmandatory governmental service, the person's specific purpose presumptively establishes the Originating Informational Purpose. The interaction does not constitute generalized consent to materially unrelated governmental inquiry, correlation, inference, retention, or reuse.

(h) Purpose Divergence

A materially divergent governmental identity use requires independently sufficient Positive Legal Authority and compliance with PDTA requirements governing Legitimate Informational Authority, Purpose Divergence, Informational Justification Level, Materially Renewed Authorization, and structural limitation of capability.

Digital Autonomy does not require government to obtain consent for an informational act supported by independently sufficient governmental authority. Conversely, a person's use of a digital service, Credential, portal, or identity mechanism does not constitute consent to unrelated governmental informational activity.

SECTION 6. IDENTITY OPERATIONS AND GOVERNMENTAL INFORMATIONAL AUTHORITY

(a) Separate Operations

Identification, Authentication, Technical Authorization, Attribute Verification, Identity Resolution, Credential Issuance, Credential Presentation, Eligibility Determination, correlation, inference, and disclosure are distinct informational operations.

(b) No Implied Authority

Authority to perform one operation does not imply authority to perform another.

(c) Purpose

Each material governmental identity operation SHALL be associated with an Originating Informational Purpose and sufficient Governmental Informational Authority under PDTA.

(d) Material Expansion

A materially broader identity operation requires materially renewed authorization as required by PDTA.

(e) Standing Capability

Standing Technical Informational Capability SHALL correspond to, and SHALL NOT materially exceed, Necessary Standing Informational Capability. Necessary Standing Informational Capability SHALL remain within Standing Legitimate Informational Authority. Government SHALL NOT maintain materially broader ordinary standing identity capability merely because the broader capability is positively authorized, commercially bundled, technically convenient, or could lawfully be authorized for a materially different future circumstance.

(f) Structural Least Power

Before applying graduated Informational Justification Level to a proposed identity capability, a Government Agency SHALL determine whether a materially less informationally powerful architecture can reasonably perform the legitimate function. Materially broader capability MAY become available only when the governmental relationship, predicate, purpose, and authority have expanded sufficiently to justify that capability and the broader capability is reasonably necessary to perform the resulting legitimate function.

Government SHALL NOT maintain materially broader Standing Technical Capability merely because the same capability could lawfully be authorized in a future case.

SECTION 7. IDENTIFICATION AND IDENTITY RESOLUTION

(a) Identification

Government may identify a person or entity where Identification is reasonably necessary and supported by authority sufficient for the governmental purpose.

(b) Identity Resolution as Separate Operation

Possession of records, Identifiers, Credentials, accounts, device information, or other information does not itself authorize Identity Resolution.

(c) Material Identity Resolution

Where Identity Resolution materially expands governmental individualized or relational knowledge, the operation SHALL satisfy PDTA requirements governing Positive Legal Authority, Legitimate Informational Authority, Material Expansion, Purpose Divergence, purpose and Question Particularity, necessity, correlation, inference, discovery, permitted consequence, and Structural Least Power.

Where Identity Resolution materially expands governmental individualized or relational knowledge, the operation SHALL satisfy PDTA requirements governing Material Expansion, purpose, particularity, necessity, correlation, inference, discovery, and permitted consequence.

(d) No Voluntary-Presentation Requirement for Lawful Government Functions

Nothing in this Act requires active Credential Presentation as the exclusive lawful method by which government may identify a person.

(e) Anti-Correlation Design

Where a governmental function does not require cross-context Identity Resolution, the architecture **SHALL**, where reasonably practicable, avoid Identifiers or mechanisms that make such resolution available through ordinary Standing Technical Informational Capability. A common Identifier, interoperable trust framework, shared status service, or technically available resolution service does not itself justify generalized Identity Resolution capability.

Where a governmental function does not require cross-context Identity Resolution, the architecture shall, where reasonably practicable, avoid Identifiers or mechanisms that make such resolution available through ordinary Standing Technical Capability.

SECTION 8. AUTHENTICATION AND AUTHORIZATION

(a) Authentication Does Not Create Authority

Successful Authentication establishes only what the Authentication process is designed and authorized to establish. Authentication does not itself authorize government to retrieve, correlate, infer from, disclose, or retain additional information.

(b) Technical Authorization Context

A material technical authorization decision involving Individual Information or Relational Information shall account for, as applicable: IDENTITY OR ACTOR + GOVERNMENTAL FUNCTION + PURPOSE + GOVERNMENTAL INFORMATIONAL AUTHORITY + AUTHORIZED OBJECT + INFORMATION DOMAIN + INFORMATIONAL OPERATION + PREDICATE + DURATION + PERMITTED CONSEQUENCE.

(c) Purpose-Bound Technical Authorization

Technical Authorization **SHALL** be bounded to the governmental function and information necessary for the authorized operation and **SHALL** operate only within independently sufficient Governmental Informational Authority.

(d) No Universal Administrative Technical Authorization

No identity or access-management architecture may create unrestricted ordinary administrative access to all identity domains or associated information. Exceptional administrative capability is governed by Section 18.

SECTION 9. CREDENTIAL ISSUANCE, HOLDING, PRESENTATION, AND DELEGATION

(a) Credential Issuance

A Government Agency may issue or recognize a Credential where reasonably related to a lawful governmental function.

(b) Holder-Controlled Environment

Where reasonably practicable, an individually usable Credential shall be capable of being maintained and presented through a Holder-Controlled Credential Environment.

(c) No Mandatory Smartphone

No person shall be required to possess a smartphone as the exclusive means of holding or presenting a government-required Credential.

(d) Delegation

Credential architecture SHALL support lawful delegation through Authorized Information Trustees where appropriate.

(e) Guardianship

Credential systems used by minors, protected persons, or persons acting through guardians SHALL support lawful guardianship while preserving the person's dignity, privacy, developmental capacity, and restoration of control where legally appropriate.

(f) Portability

Government-issued Credentials intended for individual use SHALL support reasonable portability among conforming Credential Wallets or other conforming environments where technically practicable. Portability may be satisfied through secure export, re-binding, re-provisioning, or reissuance and does not require export of non-exportable private keys, circumvention of hardware-backed security, or weakening of Credential assurance.

(g) No Government Golden Record

The fact that government issues or recognizes Credentials does not authorize government to maintain a comprehensive repository of every Credential, presentation, transaction, or attribute associated with each person.

SECTION 10. AUTHORIZED ANSWER AND VERIFICATION BEFORE COLLECTION

(a) Authorized Answer Principle

Where government is authorized to establish whether a defined proposition is true but possession of the underlying information is not independently necessary, the architecture SHALL, where reasonably practicable, permit government to obtain the Authorized Answer without acquiring the underlying information. An Authorized Answer or derived-attribute pattern SHALL be used where it materially reduces governmental knowledge without defeating the lawful function and is reasonably practicable in light of subsection (d).

Where government is authorized to establish whether a defined proposition is true but possession of the underlying information is not independently necessary, the architecture shall, where reasonably practicable, permit government to obtain the authorized answer without acquiring the underlying information.

(b) Verification Presumption

Where Attribute Verification can reasonably satisfy the governmental purpose, government shall use Verification rather than collection of the underlying information unless the Government Agency documents an independently sufficient need for the underlying information.

(c) Collection Instead of Verification

Where government collects underlying information despite a reasonably practicable Verification alternative, the Government Agency SHALL document the reason collection was reasonably necessary.

(d) Factors

(1) applicable law;

- (2) evidentiary requirements;
- (3) due process and contestability;
- (4) fraud prevention;
- (5) records requirements;
- (6) operational reliability;
- (7) security;
- (8) technical feasibility;
- (9) cost reasonably proportionate to the privacy benefit;
- (10) accessibility; and
- (11) the consequence of an erroneous Verification.

(e) No Verification Evasion

Government SHALL NOT design a transaction to require unnecessary collection merely to avoid a reasonably practicable privacy-preserving Verification method.

SECTION 11. NO-PHONE-HOME AND PRESENTATION PRIVACY

(a) General Rule

Ordinary Credential Presentation or Verification SHALL NOT require or cause communication enabling an issuer, identity provider, Credential Wallet Provider, intermediary, Government Agency not otherwise participating in the transaction, or other unrelated entity to learn that the presentation occurred, identify the Relying Party, determine the purpose of presentation, correlate presentations, construct a presentation history, or track the person across transactions, unless the communication is independently necessary and authorized for the specific transaction. Observability beyond the transaction's Necessary Standing Informational Capability constitutes Purpose Divergence and requires independent justification under PDTA.

Ordinary Credential Presentation or Verification SHALL NOT require or cause communication enabling an issuer, Credential Wallet Provider, intermediary, Government Agency not otherwise participating in the transaction, or other unrelated entity to learn that the presentation occurred, identify the Relying Party, determine the purpose of presentation, correlate presentations, construct a presentation history, or track the person across transactions, unless the communication is independently necessary and authorized for the specific transaction.

(b) Permitted Status, Authenticity, Fraud, and Security Communication

Communication with an issuer or status service may occur where reasonably necessary to establish Credential authenticity, current status, suspension, revocation, fraud indicators, or transaction security and where the communication is consistent with the authority or participation basis governing the transaction. Such communication SHALL disclose no more information than reasonably necessary and SHALL NOT be retained, correlated, or reused to construct an unrelated presentation history or cross-context profile.

(c) Privacy-Preserving Status Design

Status, suspension, expiration, or revocation mechanisms SHALL be designed, where reasonably practicable, to minimize disclosure of presentation events to issuers or intermediaries.

(d) Offline Verification

Government shall, where reasonably practicable and appropriate to the Credential and governmental function, support offline or non-observing Verification.

(e) No Consent Cure

A system whose ordinary designed operation creates unnecessary cross-context presentation surveillance does not become conforming merely because a user is presented with a generalized consent notice.

SECTION 12. SELECTIVE DISCLOSURE AND MINIMUM KNOWLEDGE EXPOSURE

(a) Minimum Knowledge

Government SHALL structure identity transactions to minimize Knowledge Exposure consistent with the governmental purpose.

(b) Selective Disclosure

Where a Credential contains information beyond what the governmental function requires, the system SHALL, where reasonably practicable, support Selective Disclosure, an Authorized Answer, a derived-attribute proof, or a functionally equivalent mechanism that materially reduces governmental knowledge without defeating the lawful function.

Where a Credential contains information beyond what the governmental function requires, the system shall, where reasonably practicable, support Selective Disclosure or a functionally equivalent mechanism.

(c) Predicate Answers

Where the relevant question is whether a predicate is satisfied, government shall avoid collecting the underlying value unless the Government Agency establishes that the underlying value is independently necessary. Examples include whether a person exceeds a legally relevant age; whether a license is valid; whether residency is established; whether an authorization remains active; or whether eligibility criteria are satisfied.

(d) No Hidden Expansion

A Verification transaction SHALL NOT silently authorize acquisition of additional attributes available to the Verifier but unnecessary to the transaction.

SECTION 13. PURPOSE SEQUESTRATION AND PROHIBITION ON GOVERNMENT POPULATION GOLDEN RECORDS

(a) Purpose Sequestration

Identity infrastructure SHALL preserve materially meaningful boundaries among governmental purposes. Purpose Sequestration may be logical, cryptographic, organizational, physical, or a combination thereof.

(b) Government Population Golden Record

A Government Agency SHALL NOT design, procure, operate, fund, or materially expand identity infrastructure that creates a Government Population Golden Record prohibited by PDTA.

(c) Functional Integration

Subsection (b) applies regardless of whether generalized capability arises through centralized databases; data warehouses or lakes; master identity indexes; common Identifiers; federated query; application programming interfaces; enterprise search; identity graphs; knowledge graphs; metadata; data virtualization; commercial information services; artificial intelligence; shared administrative interfaces; or other functional integration.

(d) Functional Universal Search

Government SHALL NOT maintain Functional Universal Search through identity infrastructure.

(e) Judicial Authorization

Judicial authorization of a particular informational act does not itself authorize construction or maintenance of a prohibited standing identity architecture.

SECTION 14. INTEROPERABILITY WITHOUT INTEGRATION

(a) General Rule

Government systems may interoperate to complete authorized transactions without creating standing reciprocal access to underlying information.

(b) No Aggregation of Authority

Technical interoperability does not aggregate the separate Governmental Informational Authority of participating entities.

(c) Transactional Exchange

Interoperable exchanges shall be structured as bounded transactions specifying governmental purpose, participating actors, authority, information or proposition requested, permitted operation, duration, permitted consequence, and accountability.

(d) Verification Across Domains

Where one agency or government possesses authority to attest to a fact and another possesses authority to verify that fact, interoperability shall, where reasonably practicable, permit Verification without automatically transferring the underlying source record.

(e) No Integration by Federation

Federation does not constitute compliance where the resulting query layer creates substantially the same standing generalized capability as a prohibited integrated environment.

SECTION 15. IDENTIFIERS AND ANTI-CORRELATION ARCHITECTURE

(a) Contextual Assessment

No Identifier is categorically required or prohibited solely because it is universal, decentralized, centralized, persistent, pairwise, cryptographic, or otherwise characterized.

(b) Correlation Risk

Government SHALL evaluate whether an Identifier materially reduces Authorization Friction or enables unauthorized cross-purpose reconstruction.

(c) Pairwise and Purpose-Specific Identifiers

Where a universal Identifier is unnecessary to the governmental function, systems shall, where reasonably practicable, support Pairwise Identifiers, purpose-specific Identifiers, pseudonymous identifiers, or other mechanisms reducing unnecessary correlation.

(d) Universal Identifiers

A universal or persistent Identifier may be used where reasonably necessary to a legitimate governmental function and where its use does not create unauthorized generalized informational capability.

(e) Circumvention

Government SHALL NOT use Identity Resolution, commercial data, artificial intelligence, device Identifiers, metadata, or other mechanisms to defeat an anti-correlation design for a purpose not independently authorized.

SECTION 16. TRUST, AUTHENTICITY, STATUS, REVOCATION, AND EVENT INTEGRITY

(a) Authenticity

Government identity systems SHALL provide assurance appropriate to the governmental consequence concerning authenticity, integrity, issuer authority, and Credential status.

(b) Cryptographic Methods

Cryptographic signatures, proofs, key-based authentication, or equivalent methods shall be used where reasonably appropriate to establish authenticity without unnecessary informational disclosure.

(c) Technology Neutrality

Nothing in this Act mandates a specific cryptographic algorithm, Credential format, decentralized identifier method, distributed ledger, Wallet implementation, or standards organization.

(d) Event Integrity

Systems SHALL maintain sufficient Event Integrity to establish material Credential and Identifier lifecycle events.

(e) Revocation and Suspension

Revocation and suspension mechanisms SHALL be reliable; timely relative to risk; auditable; resistant to unauthorized modification; and designed to minimize unnecessary presentation surveillance.

(f) Synthetic Identity and Impersonation

Government SHALL NOT rely solely upon readily forgeable visual, audio, or other media where the governmental consequence reasonably requires stronger authenticity. GAAFA governs additional requirements concerning synthetic media and artificial intelligence.

(g) Trust Infrastructure Transparency

Material public trust, status, or Verification infrastructure used by the State SHALL be sufficiently documented and publicly auditable to permit evaluation of issuer authority, governance, material conformance, and continuity without requiring disclosure of information that would create a specific security vulnerability. No private entity shall possess exclusive control over the only

technically or legally available trust infrastructure for a statewide identity function unless the Legislature specifically authorizes the arrangement and safeguards continuity, portability, competition, and public accountability.

SECTION 17. OPEN STANDARDS, PORTABILITY, AND VENDOR INDEPENDENCE

(a) Open Standards

Government identity infrastructure shall use Open Standards where reasonably practicable.

(b) Interoperability

Government SHALL avoid unnecessary proprietary barriers preventing conforming Credentials, Wallets, Verifiers, or other components from interoperating.

(c) Portability

Individuals SHALL be able to move portable Credentials and associated user-controlled information between conforming providers where technically practicable without forfeiting substantive legal validity solely because of provider change. Portability may be accomplished through secure export, transfer, re-binding, or reissuance and need not require transfer of non-exportable cryptographic secrets.

(d) No Vendor Lock-In

Procurement SHALL avoid contractual or technical terms that make government materially dependent upon a vendor for access to governmental Credentials, keys, schemas, trust information, or records necessary for continuity.

(e) Exit Capability

Material identity procurements SHALL include reasonable provisions for data and Credential portability; key and trust transition; documentation; schema portability; interface continuity; termination assistance; and secure deletion of vendor-held information when authority expires.

SECTION 18. ADMINISTRATIVE, RECOVERY, GUARDIANSHIP, AND BREAK-GLASS CAPABILITY

(a) No Universal Administrator

Identity infrastructure SHALL NOT provide ordinary administrative users unrestricted capability to access, impersonate, correlate, export, or reconstruct all individual identity information.

(b) Administrative Privilege

Administrative privilege is technical authority and does not itself constitute Governmental Informational Authority.

(c) Recovery

Systems SHALL provide proportionate mechanisms for Credential, key, account, and identity recovery where necessary. Recovery mechanisms shall, where reasonably practicable, avoid population-scale master secrets or universal backdoors.

(d) Authorized Information Trustees

Recovery and delegated administration MAY use Authorized Information Trustees consistent with PDTA.

(e) Break Glass

Exceptional access SHALL specify purpose, authority, trigger, actor, scope, permitted operation, duration, audit, termination, and post-event review.

(e-1) Exception Envelope

Break-glass, recovery, emergency, and other exceptional identity capability SHALL be implemented within the PDTA Exception Envelope, including PDTA's invocation-specific activation and immediate-emergency rules. The envelope SHALL identify the identity-specific Credential, Identifier, information domains, Technical Authorization, permitted informational operations, duration, audit, and termination conditions applicable to the exceptional access. A preapproved identity exception does not itself create standing Technical Authorization or Governmental Informational Authority.

(f) Expiration

Exceptional access SHALL terminate when the authority supporting it expires.

SECTION 19. INTEGRATED DIGITAL SERVICE DELIVERY AND ORCHESTRATION

(a) Integrated Experience

Government may provide integrated portals, common service entry points, no-wrong-door services, or other coordinated digital experiences.

(b) No Merger of Authority

An integrated user experience does not merge the informational authority of participating programs.

(c) Citizen-Originated Service Flow

Where a person initiates a request for governmental service, the architecture SHALL treat the person's specific requested service as the presumptive Citizen-Originated Purpose and, as appropriate to the governmental function: identify the requested service; explain material eligibility or legal prerequisites; determine the facts or propositions reasonably necessary; use Verification or an Authorized Answer where reasonably practicable; collect only information independently necessary; apply applicable program rules; inform the person of material deficiencies where disclosure is lawful; complete the governmental transaction; issue a Credential or other proof where appropriate; and retain information only under applicable authority. The person's initiation of the service does not authorize materially divergent governmental use.

Where a person initiates a request for governmental service, the architecture shall, as appropriate to the governmental function: identify the requested service; establish the Citizen-Originated Purpose; explain material eligibility or legal prerequisites; determine the facts or propositions reasonably necessary; use Verification where reasonably practicable; collect only information independently necessary; apply applicable program rules; inform the person of material

deficiencies where disclosure is lawful; complete the governmental transaction; issue a Credential or other proof where appropriate; and retain information only under applicable authority.

(d) Orchestration Minimization

An orchestration layer SHALL NOT obtain, retain, or expose information from participating programs merely because the information is technically available.

(e) Purpose Composition

Where a user requests multiple governmental services, each participating governmental purpose retains its own informational boundary unless lawful Purpose Composition under PDTA authorizes coordination.

(f) No-Wrong-Door Principle

Service integration does not require governmental informational integration.

(g) Composite Service Transactions

Where an integrated digital service or orchestration flow spans multiple agencies, programs, identity providers, Vendors, or automated systems, the flow is a Composite Governmental Information Transaction under PDTA. The participating entities SHALL identify the Responsible Government Agency where required by PDTA and SHALL preserve the separate authority of each participating governmental purpose. Neither composite assessment nor Responsible Government Agency designation merges program authority, creates a common identity purpose, or gives a shared-service operator substantive access beyond independently sufficient authority. Layered responsibility may be used for shared identity infrastructure consistent with PDTA.

SECTION 20. ACCESSIBILITY, NONDIGITAL EQUIVALENCE, AND DIGITAL INCLUSION

(a) Equal Legal Access

Government SHALL provide a reasonably accessible means for persons to exercise legal rights and obtain governmental services regardless of ability to use a particular digital identity technology.

(b) No Mandatory Device

Government SHALL NOT make smartphone ownership, a particular operating system, broadband access, a commercial Wallet, or similar technology an exclusive prerequisite to a governmental right or generally available service unless expressly required by law and reasonably necessary.

(c) Biometric Authentication and Identification

Government SHALL NOT require biometric enrollment merely because a digital system supports biometrics. Device-local or holder-controlled biometric authentication that does not disclose a reusable biometric template to government may be used where appropriate to secure a Credential or device. Centralized biometric collection, repository maintenance, one-to-many identification, or population-scale matching requires independently sufficient authority and a documented assessment of purpose, necessity, matching scope, retention, security, error consequences, and reasonably available less-intrusive alternatives.

(d) Assisted Access

Government SHALL provide reasonable assisted-service mechanisms for persons requiring accessibility, language, disability, guardianship, or digital-literacy support.

(e) Informational Equivalence

Alternative service channels SHALL NOT require materially greater disclosure merely because the individual uses a nondigital or assisted channel, except where reasonably necessary to the channel, legal requirement, or security risk. A material increase in information collection SHALL be documented and minimized.

(f) Functional Equivalence

Alternative channels need not use identical technology but SHALL provide functionally equivalent legal access and reasonably comparable informational protection.

**SECTION 21. INTERGOVERNMENTAL AND CROSS-SOVEREIGN IDENTITY
TRANSACTIONS**

(a) Inter-Sovereign Boundary

Information or identity authority available to one sovereign or governmental entity does not become generally available to another merely because technical interoperability exists.

(b) Independent Authority

A receiving governmental entity SHALL possess independently sufficient authority for the informational operation it performs.

(c) Verification

Where reasonably practicable, cross-sovereign transactions shall verify required facts without transferring underlying source records.

(d) No Authority Aggregation

Participating governments SHALL NOT aggregate their separate authorities into collective generalized informational power.

(e) Capability Laundering

A Government Agency SHALL NOT use another government, fusion environment, shared service, interstate system, federal service, or other governmental partner to obtain capability that the Agency could not lawfully maintain or exercise directly.

(f) Trust Recognition

Nothing in this section prevents recognition of Credentials issued by another jurisdiction where authenticity, issuer authority, and required claims can be established.

(g) Nondiscrimination and Reciprocal Recognition

State recognition or Certification rules SHALL apply on a facially nondiscriminatory basis to similarly situated in-state and out-of-state issuers, Wallet providers, Verifiers, and Relying Parties. Mutual recognition with another jurisdiction occurs only to the extent that each participating jurisdiction has lawfully adopted reciprocal or substantially equivalent recognition. Nothing in this Act purports to impose Certification obligations upon transactions lacking a material nexus to this State or its Government-Recognized Identity Ecosystem.

SECTION 22. VENDORS AND GOVERNMENT CONTRACTORS

(a) Governmental Responsibility

Government remains the governmental fiduciary under PDTA and remains responsible for identity capability exercised through Vendors, contractors, cloud providers, Credential providers, shared services, or other agents. A Vendor does not become a governmental fiduciary merely by contracting with government or providing governmental informational capability.

Government remains responsible under PDTA for identity capability exercised through vendors, contractors, cloud providers, Credential providers, shared services, or other agents.

(b) Vendor Non-Expansion

A Vendor may not provide or exercise, on government's behalf through ordinary arrangements, materially broader identity capability than government may lawfully and conformingly exercise for the governmental function. Vendor-provided capability available to government through ordinary arrangements is attributable to government for architectural and conformance assessment. This attribution does not by itself establish constitutional state action or governmental fiduciary status for the Vendor.

A vendor possesses no greater informational authority than the Government Agency for which it acts.

(c) Contract Requirements

Material identity contracts SHALL define, as applicable: governmental purpose; information domains; permitted operations; retention; subcontractors; independent use restrictions; prohibition on unauthorized aggregation, enrichment, profiling, sale, or reuse; security; audit; portability; termination; deletion; change notification; conformance; rights support; and compliance with PDTA, VIDA, GAAFA, and applicable DTA regulations.

(d) Capability Laundering

Government SHALL NOT procure or exercise prohibited informational capability indirectly through a vendor.

(e) Vendor Independent Use

(f) Source of Vendor Obligations

Vendor obligations arise from duties expressly imposed by this Act, PDTA, GAAFA where applicable, procurement requirements, contract, applicable agency principles, and other applicable law.

Government SHALL NOT use outsourcing to evade nondelegable governmental duties or informational-authority limits.

A vendor engaging in independent commercial use outside the governmental processing relationship is subject to applicable law governing that independent activity and may also be subject to Section 23 if participating in a Government-Recognized Identity Ecosystem.

SECTION 23. COMMERCIAL IDENTITY ECOSYSTEM PARTICIPATION AND CERTIFICATION

(a) Scope and Nexus

This section governs a Commercial Participant only with respect to participation in, Certification for, or transactions materially using a Government-Recognized Identity Ecosystem. Participation is voluntary unless another enacted law specifically requires participation for a defined regulated function. Nonparticipation does not prohibit a person from engaging in otherwise lawful private identity activity outside the ecosystem or from using non-certified identity services without representing them as state-certified.

(b) Program-Limited Conditions

Conditions imposed under this section SHALL define the limits, integrity, privacy, interoperability, or security of the Government-Recognized Identity Ecosystem and SHALL NOT be used as leverage to regulate a participant's unrelated lawful activity outside the ecosystem merely as a condition of Certification.

(c) Certification Administration

The State CIO shall administer Certification under objective criteria established by this Act, DTA conformance regulations, and CIO operational standards consistent with those regulations. The DTA may audit Certification decisions and has final administrative authority concerning conformance with this Act. Neither the CIO nor the DTA may create or enlarge Governmental Informational Authority through Certification.

(d) Certification Criteria

Certification criteria may address identity assurance, interoperability, security, privacy, No-Phone-Home design, Selective Disclosure, portability, accessibility, auditability, incident response, technical continuity, commercial ecosystem obligations, and other matters reasonably related to safe participation in the ecosystem.

(e) Participation Agreement

A Commercial Participant SHALL execute an Ecosystem Participation Agreement approved under this Act as a condition of Certification.

(f) Minimum Obligations

The agreement SHALL require the participant to: state the transaction purpose; request only information reasonably necessary to that purpose; use Verification rather than collection where reasonably practicable; limit retention; maintain reasonable security; avoid unauthorized sale, licensing, monetization, disclosure, profiling, or reuse; avoid unauthorized cross-context correlation; support applicable portability; provide required notices; maintain sufficient compliance records; permit authorized audits; comply with Section 24; flow applicable requirements to subcontractors; and provide an enforceable mechanism for suspension or termination of participation.

(g) Authorization

Where individual authorization may lawfully permit an otherwise restricted commercial use, authorization SHALL be specific, informed, unbundled from unrelated services, free from deceptive design, revocable where applicable, and documented.

(h) Government Non-Substitution

Commercial authorization or compliance does not satisfy or enlarge governmental authority under PDTA.

(i) Model Agreement

The State CIO, subject to DTA approval of provisions affecting statutory rights or conformance, SHALL publish a Model Ecosystem Participation Agreement designed to support reciprocal recognition by jurisdictions that have lawfully adopted substantially equivalent requirements.

(j) Certification Transparency

The State shall publish current Certification status, material Certification conditions, final suspension or revocation actions, and material public conformance findings. Trade secrets, cryptographic secrets, security-sensitive details, and proprietary information not necessary to public accountability may be protected as provided by law.

(k) Renewal and Appeal

Certification SHALL be subject to periodic renewal at intervals established by regulation. A denied, conditioned, suspended, or revoked applicant or participant is entitled to written reasons and an administrative appeal under [State Administrative Procedure Act] or other applicable law.

SECTION 24. PROHIBITED AND PRESUMPTIVELY PROHIBITED COMMERCIAL ECOSYSTEM PRACTICES

(a) Per Se Prohibited Practices

A Commercial Participant SHALL NOT: operate Credential Surveillance Infrastructure for unrelated cross-context tracking; covertly cause an issuer or intermediary to receive presentation-event information unnecessary to the transaction; sell or disclose Credential-presentation histories to a data broker, advertising network, or unrelated profiling service; deliberately circumvent Pairwise Identifiers, Selective Disclosure, pseudonymity, or other anti-correlation controls for the purpose of constructing an unrelated cross-context profile; or use ecosystem participation to obtain identity information through technical means the participant represented would not be used. Individual authorization does not cure conduct prohibited by this subsection unless another law expressly provides otherwise.

(b) Presumptively Prohibited Practices

The following are presumptively inconsistent with ecosystem participation obligations: cross-context Identity Resolution; correlation of presentation records across unrelated transactions; retention beyond the stated purpose; collection of underlying attributes where Verification was reasonably practicable; disclosure to an Independent Information Intermediary; reverse identification of pseudonymous activity; and materially unrelated profiling.

(c) Rebuttal

A participant may rebut subsection (b) by demonstrating by a preponderance of the evidence that the practice was specifically authorized by law or valid individual authorization where authorization is legally sufficient; reasonably necessary for a defined security, fraud-prevention, recovery, dispute-resolution, legal-compliance, or holder-directed purpose; proportionate in scope and duration; and not used for materially unrelated profiling or monetization.

(d) Certification Consequences and Due Process

A material violation may result in remediation conditions, suspension, or revocation of Certification after appropriate process. A knowing per se violation may support immediate temporary suspension where continued operation presents material risk, provided the participant receives prompt written notice and an opportunity for a post-suspension hearing within [10] business days or another period specified by law.

SECTION 25. ARTIFICIAL INTELLIGENCE AND AUTOMATED-SYSTEM BOUNDARY INHERITANCE

(a) No Independent Authority

Artificial intelligence, automated agents, algorithms, models, and automated identity systems possess no Governmental Informational Authority independent of the governmental actor, function, and purpose they serve.

(b) Boundary Inheritance

An automated system accessing identity infrastructure SHALL inherit all applicable purpose, authority, domain, operation, correlation, inference, retention, and consequence boundaries.

(c) No AI Circumvention

Government SHALL NOT use artificial intelligence to reconstruct, correlate, resolve, or infer identity information that a human Governmental Actor using ordinary standing authority would not be authorized to obtain.

(d) Authentication

Government MAY use automated systems to evaluate Credential authenticity, fraud indicators, or identity assurance where independently authorized.

(d-1) Relational Information

Identity Resolution, household or guardianship relationships, device or Credential associations, presentation histories, and other identity-linked relationships that constitute Relational Information remain subject to PDTA throughout verification, resolution, correlation, inference, disclosure, retention, and automated use. Identity infrastructure SHALL NOT treat relational artifacts as outside fiduciary or conformance requirements merely because no single individual exclusively controls the relationship. Conflicting relational interests arising from identity resolution, household, guardianship, device, Credential, or presentation relationships SHALL be handled under PDTA Section 19's conflicting-relational-interests rule.

(e) GAAFA

Substantive requirements governing AI models, automated decisions, risk classification, provenance, explanation, contestability, bias, model governance, and agentic systems are governed by GAAFA.

SECTION 26. PROCUREMENT AND ANTI-RENT-SEEKING REQUIREMENTS

(a) Functions, Not Generalized Capability

Government SHALL procure the least informationally powerful identity functions reasonably sufficient for the legitimate standing function, not materially broader generalized informational capability merely because broader capability is positively authorized, commercially bundled, technically convenient, or potentially useful in a future circumstance.

Government SHALL procure identity functions, not materially broader generalized informational capability merely because broader capability is bundled with the product or service.

(b) Procurement Evaluation

Material identity procurement SHALL evaluate Positive Legal Authority; Standing Legitimate Informational Authority; Necessary Standing Informational Capability; Standing Technical Informational Capability; the Authority-Capability Delta; cross-purpose search; Identity Resolution; Identifier correlation; metadata; administrator capability; Vendor independent use; AI access; commercial intermediary access; interoperability; portability; exit capability; open standards; No-Phone-Home capability; accessibility; narrower architectural alternatives; and FCGIAS conformance.

(c) Anti-Rent-Seeking

Government SHALL avoid procurement structures that unnecessarily grant exclusive control over identity infrastructure; require payment of transaction tolls for ordinary exercise of government-issued Credentials; prevent Credential portability; create proprietary dependence; require unnecessary data aggregation; or make lawful transition to another provider commercially or technically impracticable.

(d) Competition

Nothing in this Act requires government to certify an unlimited number of providers where security, interoperability, operational, or fiscal considerations reasonably justify qualification requirements, provided the criteria are objective and nondiscriminatory.

SECTION 27. DTA OVERSIGHT AND STATE CIO IMPLEMENTATION

(a) DTA

The Data Trusteeship Authority established by PDTA is the principal independent oversight and enforcement authority for this Act.

(b) State CIO

The [State Chief Information Officer or equivalent official] is responsible for operational implementation of statewide identity infrastructure, technical interoperability, procurement implementation, trust frameworks, Credential infrastructure, Certification administration, technical guidance, and other executive technology functions assigned by law.

(c) Separation of Roles

The State CIO administers and implements. The DTA independently evaluates conformance and enforces this Act. The CIO may not waive, narrow, or redefine a statutory right, duty, prohibition,

or conformance requirement. The DTA may not direct ordinary executive technology operations beyond what is reasonably necessary to determine, remedy, or enforce legal conformance.

(d) Conformance Authority

Where the CIO and DTA disagree whether a technical implementation conforms to this Act or a binding DTA regulation, the DTA's final administrative conformance determination controls, subject to judicial review under applicable law.

(d-1) Remedial and Operational Boundary

The DTA may specify the legal or conformance outcome necessary to cure nonconforming identity capability. The State CIO and Responsible Government Agency retain authority to select and operate the lawful technical implementation satisfying that outcome, subject to DTA review for conformance. Nothing in this section authorizes the DTA to assume ordinary statewide identity operations or authorizes the State CIO to waive a statutory or DTA conformance requirement.

(e) DTA Powers

The DTA may exercise the investigative, audit, testing, subpoena, remedial, and enforcement powers granted by PDTA with respect to this Act.

(f) Technical Expertise

The DTA and State CIO SHALL maintain or obtain appropriate expertise in identity, cryptography, accessibility, cybersecurity, privacy engineering, interoperability, government operations, and related fields.

(f-1) Identity-Security and Abuse-Detection Profile

Identity-security, credential-fraud, account-takeover, issuer-compromise, verifier-abuse, insider-threat, and ecosystem-integrity processing MAY correlate security telemetry across identity components only within the PDTA cybersecurity and abuse-detection profile. The profile concerns protection of identity systems, accounts, Credentials, authentication and Technical Authorization mechanisms, confidentiality, integrity, availability, and technical misuse or compromise. Such processing SHALL NOT create a generalized identity-surveillance capability or authorize reuse of presentation histories, identifiers, or relationship data for unrelated programmatic, disciplinary, eligibility, regulatory, investigative, commercial, or law-enforcement purposes. A material transition to such a substantive purpose requires the separately applicable Governmental Informational Authority and Materially Renewed Authorization where required.

(g) No Oversight Golden Record

Neither implementation nor oversight requires creation of a centralized repository of statewide identity transactions.

SECTION 28. CONFORMANCE, RULEMAKING, AND TECHNICAL STANDARDS

(a) DTA Rulemaking

The DTA may adopt binding conformance regulations implementing this Act pursuant to PDTA.

(a-1) Trilogy Conformance Code

Binding identity conformance regulations adopted under this Act SHALL be maintained within the PDTA Trilogy Conformance Code and public version registry. Identity-specific conformance

profiles may identify additional technical evidence, testing, Certification, interoperability, or accessibility requirements but SHALL remain traceable to enacted authority and the controlling Code version.

(a-2) FCGIAS Reference Integrity

Any FCGIAS identity control, reference implementation, conformance test, or technical profile used as a binding requirement SHALL be incorporated and traceable in the manner required by PDTA Section 25. FCGIAS does not independently create a mandatory identity architecture, Governmental Informational Authority, private right, exception, or Vendor obligation.

(b) CIO Technical Standards

The State CIO may issue operational technical standards consistent with this Act and DTA regulations.

(c) Normative Priority

The following hierarchy applies to a governmental identity or digital-service implementation: CONSTITUTION AND OTHER CONTROLLING ENACTED LAW → PDTA, VIDA, AND GAAFA SUBSTANTIVE REQUIREMENTS, AS APPLICABLE → DTA CONFORMANCE REGULATIONS → STATE CIO OPERATIONAL TECHNICAL STANDARDS → VENDOR AND SYSTEM IMPLEMENTATION. No lower level in this hierarchy may create Governmental Informational Authority, diminish a statutory right or duty, or authorize conduct prohibited by a controlling higher level.

(d) Technology Neutrality

Regulations and technical standards shall specify functional and conformance outcomes rather than mandate particular commercial products or protocols unless interoperability or another legitimate governmental requirement reasonably requires specification.

(e) Technical Recognition

DTA regulations and CIO guidance may recognize, approve, or describe technologies, protocols, or implementation patterns that satisfy functional requirements of this Act. Recognition of a technology does not make that technology a statutory mandate and does not exempt an implementation from capability-based conformance assessment.

(f) Conformance Testing

Conformance SHALL evaluate actual capability, including functional integration through APIs, search, Identity Resolution, metadata, AI, vendors, administrators, commercial sources, and intergovernmental services.

(g) Negative Testing

Material identity systems **SHALL** be capable of assessment through negative testing designed to determine what government cannot obtain using ordinary Standing Technical Informational Capability and whether that capability materially exceeds Necessary Standing Informational Capability. Conformance **SHALL** fail where prohibited or unnecessary standing capability remains available through ordinary access and cannot be cured by documentation, policy, encryption, or audit alone.

(h) Regulatory Non-Bootstrap and Legislative Departure

The DTA and State CIO may implement enacted legitimacy and capability criteria but may not create Governmental Informational Authority, relax Structural Least-Power requirements, or treat a technical standard as an independent source of governmental power. A later statute may expressly supersede a requirement of this Act, but broad purpose language or generalized authorization **SHALL NOT** by implication repeal, waive, or satisfy a more specific informational-legitimacy requirement.

Material identity systems **SHALL** be capable of assessment through negative testing designed to determine what government cannot obtain using ordinary Standing Technical Capability.

SECTION 29. ENFORCEMENT AND REMEDIES

(a) Governmental and Vendor Enforcement

Sections 5 through 25 of this Act are enforceable through PDTA Sections 20 through 24 to the extent the challenged provision creates or protects an individual substantive right, prohibits a governmental informational act or structural capability materially affecting the claimant, or expressly imposes a privately enforceable Vendor duty. Institutional, procurement, certification-administration, rulemaking, reporting, and oversight provisions are enforceable by the DTA, Attorney General, or other public-law mechanism unless this Act expressly creates a private right.

(b) Commercial Participant Statutory Right

A person whose identity information or Credential Presentation is processed by a Commercial Participant has a substantive statutory right to the protections established by Sections 23 and 24 with respect to that processing. A Commercial Participant's Ecosystem Participation Agreement may create additional contractual rights, and the person may be designated an intended third-party beneficiary, but contractual beneficiary status is not required to enforce the statutory rights created by this subsection.

(c) Commercial Private Right of Action

A person aggrieved by a material violation of Sections 23 or 24 may bring a civil action in [appropriate state court] against the responsible Commercial Participant, subject to the standing law of the forum. No administrative exhaustion is required unless the Legislature expressly provides otherwise.

(d) Commercial Remedies

A court may award declaratory or injunctive relief; actual damages; statutory damages of not less than [\$___] for a material or knowing violation as specified by the Legislature; reasonable attorneys' fees and costs to a prevailing plaintiff; and other equitable relief reasonably necessary

to prevent continued violation. Enhanced or punitive damages are available only where otherwise authorized by law for knowing, willful, malicious, or reckless conduct. Remedies shall avoid duplicative recovery for the same injury.

(e) Identity-Specific Structural Relief

Relief against governmental or vendor architecture may include suspension of a nonconforming identity function; removal of cross-purpose search; elimination of unnecessary issuer notification; disabling unauthorized Identity Resolution; replacement of universal correlation mechanisms; implementation of Selective Disclosure; narrowing administrative capability; restructuring interoperability; portability or migration; termination of vendor access; suspension or revocation of ecosystem Certification; and other relief necessary to bring identity capability into conformity.

(f) Least-Power Remedy

Structural relief should ordinarily follow the PDTA Least-Power Remedy principle: REMOVE CAPABILITY → NARROW CAPABILITY → TRANSACTIONALIZE → REQUIRE PREDICATE OR MATERIALLY RENEWED AUTHORIZATION → SEGREGATE OR SEQUESTER → DISABLE BUNDLED CAPABILITY → MONITOR AND AUDIT RESIDUAL CAPABILITY.

Structural relief should ordinarily follow the PDTA Least-Power Remedy principle: REMOVE CAPABILITY → NARROW CAPABILITY → TRANSACTIONALIZE → REQUIRE RENEWED AUTHORIZATION → SEGREGATE OR SEQUESTER → MONITOR AND AUDIT RESIDUAL CAPABILITY.

(g) Cumulative Rights

Nothing in this Act limits rights or remedies independently available under PDTA, GAAFA, constitutional law, civil-rights law, consumer-protection law, contract law, or other applicable law.

(h) Common Transparency and Protected Information

Public and individual transparency under this Act is governed by the common PDTA transparency and protected-information rule. Identity-specific disclosures SHALL provide sufficient information for accountability concerning material identity functions, Credential or Identifier use, responsible agencies, ecosystem participation, and available rights without requiring disclosure of cryptographic secrets, exploit-enabling security detail, protected personal or relational information, active investigative information, or other information independently protected by law. The DTA retains lawful access necessary for oversight.

SECTION 30. LEGACY SYSTEMS AND TRANSITION

(a) PDTA Transition Controls

PDTA Section 28 supplies the generally applicable transition, Legacy Structural Remediation Safe Harbor, remediation-duration, and existing-contract framework for this Act.

(b) Identity-Specific Inventory and Classification

Within the period established by PDTA or binding DTA regulation, each Government Agency SHALL identify material identity systems, Government Population Golden Record or Functional Universal Search risk, Credential Surveillance Infrastructure, cross-purpose Identity Resolution, administrator capability, Vendor dependencies, No-Phone-Home limitations, portability barriers, and other identity-specific structural nonconformance.

(c) Identity-Specific Remediation Plan

An identity-system remediation plan submitted under PDTA SHALL identify the nonconforming identity capability; lawful functions that must continue; interim safeguards; affected Credentials, Identifiers, Vendors, and interoperability dependencies; remediation milestones; and the date by which prohibited standing capability will be removed, narrowed, transactionalized, or otherwise brought into conformance.

(d) No Separate Identity Safe Harbor

This Act creates no transition period, waiver, or safe harbor independent of PDTA. A PDTA safe harbor delays only specified structural remediation and does not create Governmental Informational Authority, immunize unauthorized informational acts, or permit new or materially expanded prohibited identity capability.

(e) New and Materially Replatformed Systems

New or materially replatformed identity systems SHALL satisfy the substantive requirements of this Act upon production deployment and any structural deadline established under PDTA, except to the extent a more protective or earlier requirement applies.

(f) Contracts

Identity contracts are governed by the PDTA transition and existing-contract rules and SHALL be conformed at the earliest applicable PDTA deadline, renewal, material modification, or earlier lawful DTA requirement.

SECTION 31. PERIODIC REVIEW

(a) Consolidated Review Cycle

Review of this Act shall occur within the coordinated PDTA Section 26 trilogy review. This section does not establish a separate general review cycle.

(b) Identity-Specific Subjects

The coordinated review SHALL address Digital Autonomy; Verification Before Collection; No-Phone-Home architecture; Credential surveillance; Government Population Golden Records; Identity Resolution; Identifier correlation; Relational Information in identity systems; interoperability; commercial ecosystem participation; portability and competition; accessibility and nondigital equivalence; identity-security and abuse-detection processing; AI integration; cryptographic and identity standards; legacy remediation; intergovernmental identity exchange;

emerging circumvention mechanisms; FCGIAS reference integrity; and harmonization with PDTA and GAAFA.

(c) Stakeholder Participation

The identity portion of the coordinated review SHALL include meaningful participation by individuals, civil-liberties and privacy organizations, disability and accessibility advocates, state and local agencies, identity and cryptography experts, cybersecurity professionals, Vendors, Commercial Participants, and other materially affected stakeholders.

(d) No Automatic Sunset

The review requirement does not terminate this Act absent subsequent legislative action.

SECTION 32. SEVERABILITY

(a) General Severability

If a provision of this Act or its application to a person or circumstance is held invalid, the remaining provisions and applications remain effective to the maximum extent possible.

(b) Architectural Independence

Invalidation of a particular technical requirement does not invalidate the underlying requirements of Governmental Informational Authority, Digital Autonomy, Minimum Knowledge Exposure, Purpose Sequestration, or prohibition on generalized informational capability.

(c) Technology Independence

Invalidation or obsolescence of a particular technical implementation does not invalidate a functional statutory requirement capable of implementation through another technology.

(d) Commercial-Governmental Separation

Invalidation of a commercial ecosystem requirement does not invalidate requirements governing Government Agencies, and vice versa.

(e) Constitutional Avoidance

Where reasonably possible, this Act shall be construed to avoid constitutional invalidity while preserving its substantive purposes.

SECTION 33. EFFECTIVE DATE

(a) General Effective Date

This Act takes effect [180] days after enactment.

(b) Rulemaking and Organizational Authority

The DTA and State CIO may undertake rulemaking, planning, procurement preparation, inventories, standards development, stakeholder engagement, and other implementation activities immediately upon enactment.

(c) Transactional Duties

Transactional duties capable of immediate compliance become enforceable on the general effective date.

(d) Structural Transition

Structural transition is governed by Section 30 and PDTA.

(e) No Grandfathered Authority

No legacy system, contract, architecture, Identifier, Credential framework, or technical capability acquires Governmental Informational Authority merely because it existed before enactment.

GOVERNING CONSTRUCTION

Authentication does not create informational authority.

An Identifier does not create correlation authority.

Interoperability does not aggregate governmental authority.

Verification should provide the answer government is authorized to obtain without automatically transferring the informational environment from which the answer is derived.

Service integration does not require governmental informational integration.

Decentralization is an implementation architecture, not a substitute for authority limitation.

Artificial intelligence may exercise governmental informational capability; it does not create governmental informational authority.

Government should procure identity functions, not generalized informational power.

Digital architecture should preserve the boundaries that law places upon governmental authority rather than silently erase them.

Positive Legal Authority is necessary but is not self-validating as to the legitimacy or necessity of every standing informational capability.

Standing Technical Informational Capability SHALL NOT materially exceed Necessary Standing Informational Capability, and Necessary Standing Informational Capability SHALL remain within Standing Legitimate Informational Authority.

Authority is an outer ceiling on governmental informational power, not a specification for the maximum capability government should procure or maintain as ordinary standing power.

No Phone Home is a canonical application of Structural Least Power: where Verification can occur without unnecessary issuer, identity-provider, intermediary, or unrelated governmental observability, that observational capability should be technically unavailable absent an independently justified legitimate function.

APPENDIX A - SECTION-LEVEL FCGIAS / PDTA TRACEABILITY

This appendix is a legislative traceability aid. It does not independently create substantive law. It identifies the principal FCGIAS Version 2.2 Candidate Standard, including the adopted IR-01 clarification, and PDTA Version 2.2 concepts implemented by each VIDA section.

Version 2.2 Supplemental Traceability

T-61 through T-63 → Sections 4, 5, 7, 8, 10, 12, 14, 21, 25, and 26: PLA/LIA separation, Citizen-Originated Purpose, and bounded identity transactions.

T-64 through T-66 → Sections 7, 8, 10, 12, 14, and 21: Purpose Divergence, Informational Justification Level, and Anti-Abstraction.

T-67 through T-69 → Sections 4, 14, 21, 25, and 26: no positive-authority bootstrap, relational legitimacy, and conformance-legality separation.

T-70 / CF-79 / SD-13 → Sections 4, 7, 10, 12, 14, 25, and 26: Necessary Standing Informational Capability, Structural Least Power, No Phone Home, and procurement controls.

VIDA §	Subject	Principal FCGIAS 2.2 concepts	Principal PDTA 2.2 link
1	Short Title	-	PDTA trilogy identity statute
2	Findings/Purpose	Revised ACCP; OIA; Structural Least Power; Golden Record; authorization friction	PDTA §§ 2, 6, 8, 19
3	Definitions	Identity operation ontology; capability terms	PDTA §3
4	Trilogy Relationship	Normative hierarchy; no implied authority	PDTA §§24-25
5	Digital Autonomy	PIT; Citizen-Originated Purpose; Purpose Divergence; bounded consent	PDTA §§ 4, 6, 15
6	Identity Operations	PLA/LIA; Necessary Standing Informational Capability; Material Expansion; revised ACCP	PDTA §§ 6, 8-10
7	Identification/Resolution	Authorized Object; correlation/inference; BGD	PDTA §§8-11
8	Authentication/Authorization	Authorization transaction; no admin backdoor	PDTA §§6,19
9	Credentials	PIT/AIT; portability; anti-Golden Record	PDTA §§15-17,19
10	Authorized Answer	Verification before collection; minimum	PDTA §§7,13

		exposure	
11	No-Phone-Home	No Phone Home; Structural Least Power; metadata minimization; anti-surveillance	PDTA §§ 7, 14, 19
12	Selective Disclosure	Minimum Knowledge Exposure; Duty of Care	PDTA §§7,15
13	Purpose Sequestration	Government Golden Record; standing capability test	PDTA §§6,14,19
14	Interoperability	Transactional interoperability; no functional integration	PDTA §§6,17,19
15	Identifiers	Universal identifier contextual test; anti-correlation	PDTA §§8-10,19
16	Trust/Status/Event Integrity	Provenance; audit; technical neutrality	PDTA §§7,19,25
17	Open Standards/Portability	AIT anti-recentralization; procurement portability	PDTA §§16-17,19
18	Admin/Recovery	Admin privilege; break glass; recovery current authority	PDTA §§18-19
19	Integrated Services	Purpose Composition; orchestration minimization	PDTA §§6,9,13,19
20	Accessibility/Biometrics	No convenience exception; bounded collection	PDTA §§7,15,19
21	Intergovernmental	Inter-sovereign boundary; capability laundering	PDTA §§17,24
22	Vendors	Vendor Non-Expansion; outsourced capability attribution; nondelegable government duty	PDTA §§ 12, 17, 19
23	Commercial Ecosystem	Bounded private participation; anti-recentralization	PDTA §§12,17,24
24	Commercial Prohibitions	Credential surveillance; correlation controls	PDTA §§12,14
25	AI Boundary Inheritance	AI boundary inheritance; no AI authority	PDTA §§10,17,24
26	Procurement	Necessary Standing Informational	PDTA §§ 19, 25

		Capability; functions not generalized capability; no bundled excess	
27	DTA/CIO	Independent conformance; implementation separation	PDTA §§23,25
28	Conformance/ Standards	CF-79; negative testing; regulatory non-bootstrap; structural noncompensability	PDTA §§ 19, 25
29	Enforcement	Least-Power Remedy; structural injunctions; SD-13	PDTA §§ 21-23
30	Legacy Transition	Legacy remediation; no grandfathered authority	PDTA §28
31	Periodic Review	Continuous conformance; technology change	PDTA §§25-26
32	Severability	D4 independence; technology independence	PDTA §27
33	Effective Date	Transactional vs structural transition	PDTA §28