Kirk A. Cullimore proposes the following substitute bill:

State-Endorsed Digital Identity Program Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Kirk A. Cullimore

House Sponsor: Paul A. Cutler

LONG TITLE

General Description:

This bill creates the State-Endorsed Digital Identity Program.

Highlighted Provisions:

This bill:

- defines terms;
- establishes a digital identity bill of rights;
- creates the State-Endorsed Digital Identity Program within the Department of Government Operations;
- establishes requirements for state-endorsed digital identities;
- establishes application and eligibility requirements for obtaining a state-endorsed digital identity;
- establishes identity proofing standards;
- establishes requirements for governmental entities, health care providers, digital wallet providers, verifiers, and relying parties;
- creates a duty of loyalty related to processing identity attributes;
- provides for complaint and enforcement procedures;
- provides for a one-time audit by the Office of the Legislative Auditor General;
- provides for severability; and
- makes technical and conforming changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

63A-19-501, as last amended by Laws of Utah 2025, Chapter 475

ENACTS:

63A-20-101, Utah Code Annotated 1953

63A-20-201, Utah Code Annotated 1953

63A-20-202, Utah Code Annotated 1953

63A-20-203, Utah Code Annotated 1953

63A-20-301, Utah Code Annotated 1953

63A-20-302, Utah Code Annotated 1953

63A-20-303, Utah Code Annotated 1953

63A-20-304, Utah Code Annotated 1953

63A-20-305, Utah Code Annotated 1953

63A-20-401, Utah Code Annotated 1953

63A-20-501, Utah Code Annotated 1953

63A-20-601, Utah Code Annotated 1953

63A-20-701, Utah Code Annotated 1953

63A-20-702, Utah Code Annotated 1953

63A-20-801, Utah Code Annotated 1953

63A-20-802, Utah Code Annotated 1953

63A-20-901, Utah Code Annotated 1953

REPEALS:

63A-16-1201, as enacted by Laws of Utah 2025, Chapter 352

63A-16-1202, as enacted by Laws of Utah 2025, Chapter 352

63A-16-1203, as enacted by Laws of Utah 2025, Chapter 352

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **63A-19-501** is amended to read:

63A-19-501 . Data privacy ombudsperson.

(1) The governor shall appoint a data privacy ombudsperson with the advice of the governing board.

(2) The ombudsperson shall:

(a) be familiar with the provisions of:

(i) this chapter;

(ii) Chapter 12, Division of Archives and Records Service and Management of Government Records;

(iii) Chapter 20, State-Endorsed Digital Identity; and

[~~(iii)~~] (iv) Title 63G, Chapter 2, Government Records Access and Management Act; and

(b) serve as a resource for:

(i) an individual who is making or responding to a complaint about a governmental entity's data privacy practice; and

(ii) a governmental entity which is the subject of a data privacy complaint.

(3) The ombudsperson may, upon request by a governmental entity or individual, mediate data privacy disputes between individuals and governmental entities.

(4) After consultation with the chief privacy officer, the ombudsperson may raise issues and questions before the governing board regarding serious and repeated violations of data privacy from:

(a) a specific governmental entity; or

(b) widespread governmental entity data privacy practices.

(5) When a data privacy complaint has been resolved, the ombudsperson shall post on the office's website a summary of the complaint and the resolution of the matter.

(6) The ombudsperson may receive and review complaints regarding alleged violations of Chapter 20, State-Endorsed Digital Identity, by private sector entities, and may refer such complaints to the attorney general for enforcement in accordance with Section 63A-20-801.

Section 2. Section **63A-20-101** is enacted to read:

CHAPTER 20. State-Endorsed Digital Identity

Part 1. Digital Identity Bill of Rights

63A-20-101 . Digital identity bill of rights.

The following rights constitute the digital identity bill of rights in this state:

(1) An individual possesses an individual identity innate to the individual's existence and independent of the state, which identity is fundamental and inalienable.

(2) An individual has a right to the management and control of the individual's digital identity to protect individual privacy.

(3) An individual has a right to choose, receive, and use a physical form of identity assertion that is endorsed by the state.

(4) An individual has a right to not be compelled by the state to possess, use, or rely upon a digital form of identity assertion in place of a physical form of identity assertion that is

endorsed by the state.

(5) An individual has a right to state endorsement of the individual's digital identity upon meeting objective, uniform standards for eligibility and verification established by law, and a right to not have such endorsement arbitrarily or discriminatorily withheld or revoked.

(6) An individual has a right to have the state's operation of digital identity systems governed by clear standards established by the Legislature, including for eligibility, issuance, endorsement, acceptance, revocation, or interoperability of digital identity assertions.

(7) An individual has a right to transparency in the design and operation of a state digital identity, including the right to access, read, and review the standards and technical specifications upon which the state digital identity is built and operates.

(8) An individual has the right to choose what identity attributes are disclosed by the individual's state digital identity in accordance with standards established by the Legislature.

(9) An individual has the right to any service or benefit to which the individual is otherwise lawfully entitled based on the individual's choice of a lawful format or means of identity assertion without denial, diminishment, or condition.

(10) An individual has a right to be free from surveillance, profiling, tracking, or persistent monitoring of the individual's assertions of digital identity by the state, except as authorized by law.

(11) An individual has a right to not be required by the state to surrender the individual's device in order to present the individual's digital identity.

Section 3. Section **63A-20-201** is enacted to read:

Part 2. Definitions and Program Creation

63A-20-201 . Definitions.

As used in this chapter:

(1) "Cross-context correlation" means the ability of a person to link, associate, or infer that the presentation of a state-endorsed digital identity originating with the same or another person relates to the same individual.

(2) "Data privacy ombudsperson" means the data privacy ombudsperson created in Section 63A-19-501.

(3)(a) "Digital guardian" means a person authorized to act in the best interest and on behalf of another individual.

(b) "Digital guardian" includes a:

(i) representative designated by the individual as described in the rules made by the department;

(ii) custodial parent of an unemancipated minor;

(iii) legal guardian of a minor appointed under Section 75-5-202; or

(iv) legal guardian of an incapacitated Ĥ→ [~~person~~] **individual** ←Ĥ appointed under Section 75-5-301.

(4)(a) "Digital identity" means an electronic record that:

(i) an individual may use to assert an individual's identity or identity attributes; and

(ii) can be mathematically verified.

(b) "Digital identity" does not include an electronic record that Ĥ→ **only** ←Ĥ relies on shared authentication information to verify an individual's identity, including a username, password, personal identification number, or one-time code.

(5) "Digital wallet" means an application, hardware device, software, or service that securely stores, organizes, and manages a state digital identity.

(6) "Digital wallet provider" means a person that creates, develops, maintains, supports, and makes available a digital wallet for a state digital identity.

(7) "Governmental entity" means the same as that term is defined in Section 63A-19-101.

(8) "Health care provider" means the same as that term is defined in Section 78B-3-403.

(9) "Holder" means:

(a) an individual whose identity attributes are contained in the state digital identity; or

(b) a digital guardian who manages and presents a state digital identity on behalf of the individual.

(10) "Identity" means the qualities, features, or characteristics that identify or distinguish an individual.

(11) "Identity attribute" means a specific quality, characteristic, fact, or information related to an individual's identity.

(12) "Identity proofing" means the process of collecting, validating, and verifying information about an individual to establish confidence in the individual's claimed identity.

(13) "Identity proofing entity" means an entity authorized by the department to conduct identity proofing for the purpose of issuing a state-endorsed digital identity.

(14) "Individual" means a human being.

(15) "Minor" means an individual who is under 18 years old.

(16) "Offline presentation" means a presentation that does not involve the internet.

(17) "Online presentation" means a presentation that utilizes the internet or other computer network.

(18) "Parent" means an individual who has established a parent-child relationship with a child as described in Section 81-5-201.

(19) "Person" means an individual, corporation, organization, association, governmental entity, or other legal entity.

(20) "Personal digital identifier" means an identifier that is:

(a) unique;

(b) created by or at the direction of an individual;

(c) mathematically provable to be under a holder's control; and

(d) transportable to technical infrastructure of the holder's choosing.

(21) "Physical identity" means a physical record that an individual may use to assert the individual's identity issued by:

(a) a governmental entity;

(b) the equivalent of a governmental entity in another state;

(c) the federal government; or

(d) another country.

(22) "Presentation" means the disclosure of an individual's identity attributes from the individual's state digital identity to a verifier or relying party.

(23) "Process" means any operation or set of operations performed on an individual's identity attributes.

(24) "Program" means the state-endorsed digital identity program described in Section 63A-20-202.

(25) "Program manager" means the individual appointed under Section 63A-20-203.

(26) "Relying party" means a person that relies on a verifier's assertion of an individual's identity or identity attribute that a state digital identity provides.

(27) "Secure electronic device" means a device capable of securely storing, presenting, or displaying a state-endorsed digital identity, including physical tokens and accessible devices.

(28) "State digital identity" means:

(a) a state-endorsed digital identity; or

(b) an electronic license certificate or identification card issued in accordance with

Section 53-3-235.

(29) "State-endorsed digital identity" means an individual's digital identity that:

(a) includes a personal digital identifier; and

(b) the department has issued.

(30) "Verifier" means a person that mathematically verifies a state digital identity to evaluate the state digital identity's authenticity and integrity.

Section 4. Section **63A-20-202** is enacted to read:

63A-20-202 . Digital identity program -- creation -- duties.

(1) There is created within the department the State-Endorsed Digital Identity Program.

(2) The department shall design, implement, administer, and issue a state-endorsed digital identity in compliance with the requirements in Part 3, State-Endorsed Digital Identity.

(3)(a) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the department shall make rules to:

(i) administer this chapter;

(ii) establish technological standards and best practices for governmental entities regarding:

(A) the creation, issuance, use, and acceptance of a state-endorsed digital identity; and

(B) the collection, processing, storage, and disclosure of individual identity or identity attributes; and

(iii) establish procedures for an individual to:

(A) apply for a state-endorsed digital identity; and

(B) designate a digital guardian.

(b) The department shall:

(i) accept public comment for a period of 45 days from the day the proposed rule is published in the Utah State Bulletin as described in Section 63G-3-301; and

(ii) issue a response to substantive comments submitted by the public before making the proposed rule effective.

(4) In furtherance of these duties the department may consult with:

(a) governmental entities;

(b) government entities in other states;

(c) technology experts; or

(d) organizations that establish technology standards.

(5) The department may:

(a) establish fees in accordance with Section 63J-1-504 for issuing, renewing, or replacing a state-endorsed digital identity; or

(b) apply for, accept, allocate, and administer grants, funds, or awards from any public or private source for the purpose of implementing this chapter.

(6) Beginning on January 1, 2027, the department shall annually report before June 1 to the Economic Development and Workforce Services Interim Committee regarding:

(a) program implementation and adoption metrics;

(b) security incidents and remediation steps taken in response;

(c) comments submitted to the program by the public;

(d) changes made to the program as a result of comments submitted by the public;

(e) vendor ecosystem status, including number of conformant digital wallets and verifier tools; and

(f) any recommended statutory changes.

Section 5. Section **63A-20-203** is enacted to read:

63A-20-203 . Program manager -- appointment -- duties.

(1) The executive director, with the approval of the governor, shall appoint an individual to manage the program.

(2) The program manager shall be experienced in:

(a) government administration;

(b) data privacy;

(c) cybersecurity; and

(d) information technology.

(3) The program manager is responsible for implementing a state-endorsed digital identity in accordance with this chapter.

Section 6. Section **63A-20-301** is enacted to read:

Part 3. State-Endorsed Digital Identity

63A-20-301 . State-endorsed digital identity requirements.

(1) A state-endorsed digital identity shall:

(a) incorporate state-of-the-art safeguards for protecting an individual's identity, including compromise detection, recovery mechanisms, and cross-context correlation protections;

(b) include methods to establish authenticity and integrity;

(c) be compatible with a wide variety of technological systems while maintaining strong privacy and security;

(d) support online and offline presentation;

(e) enable a holder to:

(i) selectively disclose an individual's identity attributes; or

(ii) demonstrate that the individual meets a specified minimum age without disclosing the individual's age or birth date;

(f) allow a holder to choose a digital wallet that conforms with the requirements established by the department; and

(g) be easy for a holder to adopt and use.

(2) The department shall:

(a) validate verification of an individual's identity provided by an identity proofing entity;

(b) comply with the requirements of this chapter through technological means where possible;

(c) ensure any technical infrastructure used to control the issuance or revocation of a state-endorsed digital identity is maintained within a state-controlled data center located within the state;

(d) ensure that a state-controlled data center located within the state shall use best practices in collection, processing, storage, and disclosure of all individual identity and identity attributes;

(e) select open technological standards for the creation, issuance, use, and acceptance of a state-endorsed digital identity that are:

(i) publicly available; and

(ii) free from:

(A) licensing fees; and

(B) patent restrictions;

(f) verify and endorse a specific set of identity attributes including an individual's:

(i) name;

(ii) birth date;

(iii) image; and

(iv) Utah residence address; and

(g) create a process for:

(i) a holder to:

(A) obtain, maintain, and control an individual's state-endorsed digital identity;

(B) use an individual's state-endorsed digital identity;

(C) limit access to an individual's state-endorsed digital identity and identity attributes;

(D) obtain a new state-endorsed digital identity if the individual's state-endorsed digital identity is compromised; and

(E) migrate a state-endorsed digital identity to another digital wallet compliant with this chapter;

(ii) a holder to request that an individual's identity attributes be amended or corrected; and

(iii) appointment of a digital guardian to obtain or use a state-endorsed digital identity on an individual's behalf.

(3) A state-endorsed digital identity may not include a mechanism that allows the department to monitor, surveil, or track the presentation of a state-endorsed digital identity to another entity.

(4) Information provided by an individual to the state to obtain a state-endorsed digital identity may only be:

(a) used for the purpose of issuing and managing a state-endorsed digital identity;

(b) used as authorized by the individual;

(c) retained as long as necessary to issue and manage a state-endorsed digital identity;

(d) maintained within a state-controlled data center located within the state; or

(e) disclosed to:

(i) the subject of the record or the subject's digital guardian; or

(ii) a person with a warrant or court order.

(5) The department may only revoke an individual's state-endorsed digital identity if:

(a) the state-endorsed digital identity has been compromised;

(b) the department's endorsement was:

(i) issued in error; or

(ii) based on fraudulent information; or

(c) the holder requests that the department revoke the individual's state-endorsed digital identity.

(6) The department shall report a data breach regarding individual identity or identity attributes in accordance with Section 63A-19-405.

Section 7. Section **63A-20-302** is enacted to read:

63A-20-302 . Application and eligibility for state-endorsed digital identity.

(1) An individual who is at least 18 years old, or is an emancipated minor, may apply to the

department for a state-endorsed digital identity.

(2) An individual who is under 18 years old, and is not an emancipated minor, may apply to the department for a state-endorsed digital identity only with the consent of the individual's digital guardian.

(3)(a) If an individual is unable to apply for a state-endorsed digital identity due to the individual's youth or incapacitation, the application may be made on behalf of that individual by the individual's digital guardian.

(b) A digital guardian applying on behalf of a minor or incapacitated Ĥ→ [~~**person**~~] **individual** ←Ĥ shall provide:

(i) identification, as required by the department; and

(ii) the consent of the incapacitated Ĥ→ [~~**person**~~] **individual** ←Ĥ , as required by the department.

(4) The department shall make rules, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, establishing:

(a) the form and manner of an application under this section;

(b) identity proofing requirements and procedures; and

(c) procedures for denial, correction, reissuance, and compromise recovery consistent with this part.

(5) An individual is not required to apply for or obtain a state-endorsed digital identity.

(6) To apply for Ĥ→ **or receive** ←Ĥ a state-endorsed digital identity, an applicant shall:

(a) have lawful presence in the United States;

(b) be a resident of Utah; and

(c) successfully complete the department's identity proofing process established under this part.

(7)(a) The department may not require collection of information that is not necessary to verify identity or eligibility.

(b) Required information may include, as determined by the department and documented by rule:

(i) the applicant's true and full legal name;

(ii) date of birth;

(iii) Utah residence address;

(iv) evidence of lawful presence in the United States;

(v) evidence of Utah residency; and

(vi) other information strictly necessary to complete identity proofing.

Section 8. Section **63A-20-303** is enacted to read:

63A-20-303 . Identity proofing.

(1)(a) The department shall establish and maintain identity proofing requirements for the issuance of a state-endorsed digital identity that:

(i) follow a generally accepted identity proofing standard;

(ii) are commensurate with the risks of impersonation, fraud, and misuse associated with the credential; and

(iii) are consistent with the privacy, civil liberties, and security requirements of this chapter.

(b) The identity proofing process shall be designed to establish, at a minimum, that:

(i) the applicant is a real individual;

(ii) the applicant is the individual the applicant claims to be;

(iii) the applicant's birth date is the date the applicant claims it to be; and

(iv) the applicant meets the eligibility requirements of Section 63A-20-302.

(c) The department shall ensure that the identity proofing process results in a credential that provides a level of confidence in the individual's identity that is:

(i) sufficiently robust to support reliance by governmental entities and private-sector relying parties where required by law or policy for online age assurance; and

(ii) appropriate for use in both online and offline presentations.

(d) Identity proofing processes shall be designed so that the state's endorsement:

(i) reflects verification at a point in time; and

(ii) does not require:

(A) continuous monitoring; or

(B) tracking.

(2)(a) An applicant shall provide true and accurate information as required under this part.

(b) Knowingly providing materially false information for the purpose of obtaining a state-endorsed digital identity constitutes fraud and may result in denial, revocation, and other remedies provided by law.

(3)(a) Obtaining or holding a state-endorsed digital identity does not affect an individual's physical identity documents.

(b) An individual is not required to surrender, cancel, or replace any physical identity document as a condition of applying for or holding a state-endorsed digital identity.

(4)(a) The department shall define by rule, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the identity proofing standards and processes required for issuance of a state-endorsed digital identity.

(b) The rules shall, at a minimum:

(i) specify the objectives the identity proofing process is intended to achieve;

(ii) describe the acceptable methods of identity proofing, including:

(A) in-person, remote, or hybrid methods, and the conditions under which each may be used; and

(B) minimum evidence requirements and validation methods;

(iii) align with generally accepted identity proofing practices; and

(iv) establish requirements and a process to become an identity proofing entity.

Section 9. Section **63A-20-304** is enacted to read:

63A-20-304 . Requirements for governmental entities.

(1) A governmental entity may not:

(a) convey a material benefit upon an individual for using a state digital identity instead of a physical identity;

(b) withhold services or benefits from an individual if the individual uses a physical identity or is otherwise unable to use a state digital identity; or

(c) require a holder to surrender the holder's secure electronic device in the course of a presentation.

(2)(a) A governmental entity that, on or after May 6, 2026, implements a new system that accepts a digital identity shall, within three months after the day on which the department issues the first state-endorsed digital identity, accept a state-endorsed digital identity.

(b) A governmental entity is not required to accept a state-endorsed digital identity within the time frame described in Subsection (2)(a) if the governmental entity:

(i)(A) demonstrates to the satisfaction of the department that accepting a state-endorsed digital identity at that time is not technically feasible; and

(B) provides a plan for accepting a state-endorsed digital identity as soon as feasible; or

(ii) is required by law to only accept a specific form of state digital identity.

Section 10. Section **63A-20-305** is enacted to read:

63A-20-305 . Requirements for health care providers.

(1) Within two years from the date the first state-endorsed digital identity is issued, a health

care provider that receives at least $10,000,000 a year in public funding shall accept a state-endorsed digital identity if the health care provider has a program or system that accepts a digital identity.

(2) A health care provider is not required to accept a state-endorsed digital identity within the time frame described in Subsection (1) if the health care provider:

(a)(i) demonstrates to the satisfaction of the department that accepting a state-endorsed digital identity at that time is not technically feasible; and

(ii) provides a plan for accepting a state-endorsed digital identity as soon as feasible; or

(b) is required by law to only accept a specific form of state digital identity.

Section 11. Section **63A-20-401** is enacted to read:

Part 4. Digital Wallet Providers

63A-20-401 . Requirements for digital wallet providers.

(1) A digital wallet produced by a digital wallet provider shall:

(a) incorporate state-of-the-art safeguards for protecting an individual's identity;

(b) process an individual's identity attributes in a secure manner;

(c) comply with the requirements of this part through technological means where possible;

(d) be tamper resistant;

(e) support online and offline presentation of a state-endorsed digital identity;

(f) maintain a secure log:

(i) with sufficient information for the holder to know:

(A) what identity attributes were provided; and

(B) the verifier or relying party the identity attributes were provided to;

(ii) accessible only to the holder;

(iii) exportable only by the holder; and

(iv) deletable only by the holder;

(g) enable a holder to:

(i) selectively disclose an individual's identity attributes; or

(ii) demonstrate that the individual meets a specified minimum age without disclosing the individual's age or birth date; and

(h) allow a presentation of a state-endorsed digital identity by a digital guardian.

(2) A digital wallet provider may only process an individual's identity attributes from a state digital identity if:

(a) the processing is necessary for a presentation;

(b) the holder has received conspicuous notice of:

(i) what identity attributes are collected from the state digital identity;

(ii) how the identity attributes are used;

(iii) the purpose for which the identity attributes are processed; and

(iv) how long the identity attributes are retained; and

(c) the holder consents to the processing of the individual's identity attributes.

(3) Information provided by a holder to a digital wallet provider for the purpose of creating or using a digital identity may only be:

(a) processed for the primary purpose for which the holder disclosed the information; and

(b) used, retained, sold, or shared:

(i) as expressly authorized by the holder; or

(ii) if required by law.

(4) Nothing in this section relieves a digital wallet provider from complying with the requirements of Title 13, Chapter 44, Protection of Personal Information Act, or Title 13, Chapter 61, Utah Consumer Privacy Act.

Section 12. Section **63A-20-501** is enacted to read:

Part 5. Verifiers

63A-20-501 . Requirements for verifiers.

(1) A verifier shall:

(a) incorporate state-of-the-art safeguards for protecting an individual's identity in the verification process;

(b) comply with the requirements of this part through technological means where possible;

(c) process an individual's identity attributes in a secure manner;

(d) process only the minimum identity attributes reasonably necessary to achieve a specified purpose defined by the relying party requesting the presentation; and

(e) accept a presentation Ĥ→ **of a state-endorsed digital identity** ←Ĥ by a digital guardian.

(2) A verifier may only process an individual's identity attributes from a state digital identity if:

(a) authorized by the holder;

(b) the processing is necessary for a presentation;

(c) the holder has received conspicuous notice of:

(i) what identity attributes are collected;

(ii) how the identity attributes are used;

(iii) the purpose for which the identity attributes are processed; and

(iv) how long the identity attributes are retained; and

(d) the holder consents to the processing of the identity attributes.

(3) A verifier may not require a holder to surrender the holder's secure electronic device in the course of a presentation.

(4) Nothing in this section relieves a verifier from complying with the requirements of Title 13, Chapter 44, Protection of Personal Information Act, or Title 13, Chapter 61, Utah Consumer Privacy Act.

Section 13. Section **63A-20-601** is enacted to read:

Part 6. Relying Parties

63A-20-601 . Requirements for relying parties.

(1) A relying party shall:

(a) incorporate state-of-the-art safeguards for protecting an individual's identity in the verification process;

(b) comply with the requirements of this part through technological means where possible;

(c) process an individual's identity attributes in a secure manner;

(d) process only the minimum identity attributes reasonably necessary to achieve a specified purpose; and

(e) accept a presentation Ĥ→ **of a state-endorsed digital identity** ←Ĥ by a digital guardian.

(2) A relying party may only process an individual's identity attributes from a state digital identity if:

(a) authorized by the holder;

(b) the processing is necessary for a specified purpose;

(c) the holder has received conspicuous notice of:

(i) what identity attributes are collected;

(ii) how the identity attributes are used;

(iii) the purpose for which the identity attributes are processed; and

(iv) how long the identity attributes are retained; and

(d) the holder consents to the processing of the identity attributes.

(3) A relying party may not require a holder to surrender the holder's secure electronic device in the course of a presentation.

(4) A relying party may accept a state-endorsed digital identity as proof of an individual's

identity or identity attributes unless a different method of proof is required by law.

(5) Nothing in this section relieves a relying party from complying with the requirements of Title 13, Chapter 44, Protection of Personal Information Act, or Title 13, Chapter 61, Utah Consumer Privacy Act.

Section 14. Section **63A-20-701** is enacted to read:

Part 7. General Requirements

63A-20-701 . Duty of loyalty.

The department, a digital wallet provider, a verifier, a relying party, and a digital guardian shall refrain from practices or activities related to the processing of an individual's identity attributes from a digital identity that:

(1) conflict with the best interests of an individual;

(2) take advantage of or otherwise exploit an individual;

(3) result in a disproportionate risk to an individual;

(4) are to an individual's detriment; or

(5) cause harm to an individual.

Section 15. Section **63A-20-702** is enacted to read:

63A-20-702 . Processing restrictions.

(1) Any record of a presentation of a state digital identity may only be processed by a digital wallet provider, a verifier, or a relying party:

(a) for the primary purpose for which the presentation was performed; or

(b) if required by law.

(2) Information provided by a holder, verifier, or relying party to a verifier or relying party in the course of a presentation may only be:

(a) processed for the primary purpose for which the holder disclosed the information; and

(b) used, retained, sold, or shared:

(i) following conspicuous notice to and express authorization by the holder; or

(ii) if required by law.

Section 16. Section **63A-20-801** is enacted to read:

Part 8. Enforcement and Audit

63A-20-801 . Complaints and enforcement.

(1) An individual may submit a complaint to the data privacy ombudsperson alleging a violation of this chapter by:

(a) the department;

(b) a digital wallet provider;

(c) a verifier; or

(d) a relying party.

(2) The data privacy ombudsperson may receive and review a complaint described in Subsection (1).

(3) If, after reviewing a complaint, the data privacy ombudsperson has reasonable cause to believe that a violation of this chapter has occurred, the data privacy ombudsperson may refer the complaint to the attorney general.

(4) Upon receiving a referral under Subsection (3), or when the attorney general has reasonable cause to believe that a violation of this chapter has occurred, the attorney general is authorized to:

(a) issue civil investigative demands for depositions, documents, and requests for information in the time and manner prescribed by the attorney general; and

(b) bring a civil action in a court of competent jurisdiction to:

(i) enjoin a violation of this chapter;

(ii) obtain declaratory relief regarding compliance with this chapter; or

(iii) recover damages, restitution, and disgorgement on behalf of an individual injured by a violation of this chapter.

(5) The attorney general shall treat all information received in accordance with Subsection (4) as non-public and confidential unless confidentiality is waived by the providing party, or upon the filing of an enforcement action.

(6) In an action brought under Subsection (4), the court may award:

(a) injunctive relief;

(b) declaratory relief;

(c) equitable relief including restitution and disgorgement;

(d) actual damages;

(e) costs; and

(f) reasonable attorney fees.

Section 17. Section **63A-20-802** is enacted to read:

63A-20-802 . Auditing.

(1) Subject to prioritization of the Legislative Audit Subcommittee created in Section 36-12-8, the Office of the Legislative Auditor General shall conduct an audit of the program beginning on January 1, 2028.

(2) The audit shall evaluate:

(a) the department's compliance with this chapter;

(b) whether the department has met the restrictions on monitoring, surveillance, and tracking described in Section 63A-20-301;

(c) the effectiveness of the program in meeting the objectives established in this chapter;

(d) the appropriate long-term placement of the program within state government; and

(e) recommended statutory changes to improve the program.

(3) The Office of the Legislative Auditor General shall:

(a) complete the audit report by October 31, 2028;

(b) provide the audit report to the Legislature; and

(c) present the audit findings to the Legislative Audit Subcommittee at the subcommittee's next meeting after completion of the audit report.

Section 18. Section **63A-20-901** is enacted to read:

Part 9. Severability

63A-20-901 . Severability.

(1) If any provision of this chapter or the application of any provision to any person or circumstance is held invalid by a final decision of a court of competent jurisdiction, the remainder of this chapter shall be given effect without the invalid provision or application.

(2) The provisions of this chapter are severable.

Section 19. **Repealer.**

This bill repeals:

Section **63A-16-1201, Definitions.**

Section **63A-16-1202, State digital identity policy.**

Section **63A-16-1203, Department duties.**

Section 20. **Effective Date.**

This bill takes effect on May 6, 2026.