Paul A. Cutler proposes the following substitute bill:

Electronic Records Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Paul A. Cutler

Senate Sponsor: Wayne A. Harper

LONG TITLE

General Description:

This bill modifies provisions relating to county recording of documents and digital authentication.

Highlighted Provisions:

This bill:

- defines terms;
- authorizes counties to accept digitally authenticated records;
- establishes requirements for digital authentication standards;
- requires review and approval from the State Archives before county implementation;
- requires the state archivist to establish retention and preservation standards for digital records;
- grants rulemaking authority to the state archivist in consultation with the Division of Technology Services;
- requires approval processes for counties before accepting digitally authenticated records; and
- makes technical and conforming changes.

Money Appropriated in this Bill:

None

Other Special Clauses:

None

Utah Code Sections Affected:

AMENDS:

17-71-301, as renumbered and amended by Laws of Utah 2025, First Special Session, Chapter 13

63A-12-101, as last amended by Laws of Utah 2025, Chapter 476

63A-12-104, as last amended by Laws of Utah 2025, Chapter 475

63A-16-104, as last amended by Laws of Utah 2024, Chapter 508

ENACTS:

17-71-301.5, Utah Code Annotated 1953

63A-12-117, Utah Code Annotated 1953

63A-16-215, Utah Code Annotated 1953

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

Section 1. Section **17-71-301** is amended to read:

17-71-301 . Document custody responsibility -- Compliance with County Recorder Standards Board rules -- Compliance with county appeal authority.

The county recorder:

(1) is custodian of all recorded documents, records, and associated data required by law to be recorded;

(2) shall comply with rules made by the County Recorder Standards Board under Section 63C-30-202, including rules that govern:

(a) the protection of recorded documents and records in the county recorder's custody;

(b) the electronic submission of plats, records, and other documents to the county recorder's office;

(c) the protection of privacy interests in the case of documents and records in the county recorder's custody; and

(d) the formatting, recording, and redaction of documents and records in the county recorder's custody;

(3) shall comply with the appeal authority established by the county legislative body in accordance with Section 17-71-306;[~~and~~]

(4) may adopt policies and procedures governing the office of the county recorder that do not conflict with this chapter or rules made by the County Recorder Standards Board under Section 63C-30-202[~~.~~] ; and

(5) shall comply with approval requirements described in Section 17-71-301.5 before accepting digitally authenticated records as defined in Section 17-71-301.5.

Section 2. Section **17-71-301.5** is enacted to read:

17-71-301.5 . Digital authentication of county records -- Standards and approval process.

(1) As used in this section:

(a) "Digital authentication" means a method of verifying the identity of a person and the integrity of an electronic document using tamper-evident technology that:

(i) creates a verifiable record of the authentication; and

(ii) meets standards established under Section 63A-12-117.

(b) "Digital authentication system" means the technology and procedures used to create digitally authenticated records.

(c) "Digitally authenticated record" means an electronic document that:

(i) has been authenticated using digital authentication as defined in this section;

(ii) meets the requirements established by rule under Section 63A-12-117; and

(iii) if the document is to be recorded by a county recorder, has been approved for county use in accordance with Section 17-71-301.5.

(d) "Division" means the Division of Technology Services created in Section 63A-16-103.

(e) "Records Management Committee" means the Records Management Committee created in Section 63A-12-112.

(f) "State Archives" means the Division of Archives and Records Service created in Section 63A-12-101.

(g) "Tamper-evident technology" means technology that:

(i) creates a permanent, verifiable record that allows detection of any unauthorized alteration to an electronic document after authentication; and

(ii) maintains an immutable audit trail of authentication events.

(2)(a) A county recorder may accept and record a digitally authenticated record if:

(i) the county has obtained approval under Subsection (3); and

(ii) the digitally authenticated record meets the requirements of Section 17-71-602.

(b) A county recorder that accepts digitally authenticated records shall:

(i) maintain procedures for accepting both digitally authenticated records and traditionally notarized documents;

(ii) provide public notice of the types of digital authentication the county accepts;

(iii) ensure compliance with retention requirements established by the state archivist under Section 63A-12-117; and

(iv) maintain audit trails for all digitally authenticated records accepted.

(3) Before accepting digitally authenticated records, a county shall:

(a) submit a proposal to the State Archives that describes:

(i) the digital authentication system the county proposes to use;

(ii) security measures to protect record integrity;

(iii) procedures for verification of authentication;

(iv) the types of records the county proposes to accept through digital authentication;

(v) implementation timelines and training plans;

(vi) compliance with retention schedules approved by the Records Management Committee;

(vii) preservation requirements for permanent records;

(viii) transfer procedures for records to be archived;

(ix) format specifications for long-term storage;

(x) consultation conducted with:

(A) the Title and Escrow Commission created in Section 31A-2-403;

(B) the County Recorder Standards Board created in Section 63C-30-201; and

(C) other private industry stakeholders with interests affected by the proposal; and

(xi) a summary of concerns raised during the consultations described in Subsection (3)(a)(x); and

(b) obtain approval from the state archivist in accordance with Subsection (4).

(4)(a) The state archivist shall review each county proposal submitted under Subsection (3) for:

(i) compliance with:

(A) retention schedules approved by the Records Management Committee;

(B) preservation standards for digital records established under Section 63A-12-117;

(C) transfer requirements for permanent records; and

(D) technical standards established by rule under Section 63A-12-117;

(ii) sufficiency of county resources and training for implementation; and

(iii) completeness of the consultation requirements described in Subsection (3)(a)(x) and consideration of concerns described in Subsection (3)(a)(xi).

(b) The state archivist shall consult with the division regarding technical aspects of a proposal.

(c) Before the state archivist approves a proposal, the county, with assistance from State Archives, shall present the proposal to the Records Management Committee in a public meeting that provides opportunity for public comment.

(d) The state archivist shall provide written approval or denial to the county within 45 days after the day on which the county submits a proposal under Subsection (3).

(e) If the state archivist denies a proposal, the state archivist shall provide:

(i) specific reasons for denial; and

(ii) recommendations for modification.

(f) A county may resubmit a modified proposal in accordance with this section.

(5) An approval granted under Subsection (4) is valid for three years and may be renewed upon demonstration of continued compliance with the requirements of this section.

(6) A county recorder may establish and collect fees for accepting and recording digitally authenticated records in accordance with Section 17-71-407.

Section 3. Section **63A-12-101** is amended to read:

63A-12-101 . Division of Archives and Records Service created -- Duties.

(1) There is created the Division of Archives and Records Service within the department.

(2) The state archives shall:

(a) administer the state's archives and records management programs, including storage of records, central reformatting programs, and quality control;

(b) apply fair, efficient, and economical management methods to the collection, creation, use, maintenance, retention, preservation, disclosure, and disposal of records and documents;

(c) establish standards, procedures, and techniques for the effective management and physical care of records;

(d) conduct surveys of office operations and recommend improvements in current records management practices, including the use of space, equipment, automation, and supplies used in creating, maintaining, storing, and servicing records;

(e) establish standards for the preparation of schedules providing for the retention of records of continuing value and for the prompt and orderly disposal of state records no longer possessing sufficient administrative, historical, legal, or fiscal value to warrant further retention;

(f) establish, maintain, and operate centralized reformatting lab facilities and quality control for the state;

(g) provide staff and support services to the Records Management Committee created in Section 63A-12-112 and the Government Records Office, created in Section 63A-12-202;

(h) develop training programs to assist records officers and other interested officers and employees of governmental entities to administer this chapter and Title 63G, Chapter 2, Government Records Access and Management Act;

(i) provide access to public records deposited in the archives;

(j) administer and maintain the Utah Public Notice Website established under Section 63A-16-601;

(k) provide assistance to any governmental entity in administering this chapter and Title 63G, Chapter 2, Government Records Access and Management Act;

(l) prepare forms for use by all governmental entities for a person requesting access to a record;[~~and~~]

(m) if the department operates the Division of Archives and Records Service as an internal service fund agency in accordance with Section 63A-1-109.5, submit to the Rate Committee established in Section 63A-1-114:

(i) the proposed rate schedule as required by Section 63A-1-114; and

(ii) other information or analysis requested by the Rate Committee[~~.~~] ; and

(n) establish standards for digital authentication systems and review county proposals for accepting digitally authenticated records in accordance with Section 17-71-301.5.

(3) The state archives may:

(a) establish a report and directives management program;

(b) establish a forms management program; and

(c) in accordance with Section 63A-12-101, require that an individual undergo a background check if the individual:

(i) applies to be, or currently is, an employee or volunteer of the division; and

(ii) will have direct access to a vulnerable record in the capacity described in Subsection (3)(c)(i).

(4) The executive director may direct the state archives to administer other functions or services consistent with this chapter and Title 63G, Chapter 2, Government Records Access and Management Act.

Section 4. Section **63A-12-104** is amended to read:

63A-12-104 . Rulemaking authority.

In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act:

(1) the state archivist may make rules establishing:

(a) procedures for the collection, storage, designation, classification, access, mediation for records access, and management of records under this chapter and Title 63G, Chapter 2, Government Records Access and Management Act; and

(b) procedures and standards for digital authentication systems and preservation of digitally authenticated records in accordance with Section 63A-12-117; and

(2) a governmental entity may make rules, policies, or ordinances specifying at which level within the governmental entity the requirements described in this chapter will be undertaken.

Section 5. Section **63A-12-117** is enacted to read:

63A-12-117 . Digital authentication systems -- Technical standards and requirements.

(1) As used in this section:

(a) "Digital authentication system" means technology and procedures used to create digitally authenticated records.

(b) "Digitally authenticated record" means the same as that term is defined in Section 17-71-301.5.

(c) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

(2) A governmental entity that creates or accepts digitally authenticated records shall:

(a) maintain the records in accordance with approved retention schedules;

(b) ensure records retain authentication characteristics throughout the retention period;

(c) transfer records to the state archives in accordance with state archivist requirements; and

(d) maintain data necessary for verification and preservation.

(3) The state archivist shall establish procedures for:

(a) accepting digitally authenticated permanent records;

(b) verifying authentication integrity upon transfer;

(c) long-term preservation of digital authentication characteristics; and

(d) providing public access to archived digitally authenticated records in accordance with Title 63G, Chapter 2, Government Records Access and Management Act.

(4)(a) The state archivist, in consultation with the Division of Technology Services, shall make rules, in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, establishing:

(i) technical standards for digital authentication systems, including:

(A) security requirements;

(B) authentication verification procedures;

(C) acceptable authentication methods and technologies;

(D) cybersecurity standards; and

(E) system integrity requirements;

(ii) preservation standards for digital authentication systems to ensure long-term

preservation;

(iii) retention schedule requirements for digitally authenticated records;

(iv) transfer procedures from governmental entities to state archives;

(v) format specifications for archival storage of digitally authenticated records;

(vi) verification procedures for authentication integrity; and

(vii) data requirements for preservation and access.

(b) The state archivist shall ensure that standards established under this section require digitally authenticated records to demonstrate:

(i) immutability or tamper-evident characteristics sufficient to detect unauthorized alterations;

(ii) verified identity of the person authenticating the record using identity verification procedures that meet or exceed the requirements for satisfactory evidence of identity established for remote notarization under Section 46-1-2;

(iii) format sustainability for long-term preservation; and

(iv) compliance with retention schedules.

(5) In making rules under Subsection (4), the state archivist shall consult with:

(a) the Title and Escrow Commission created in Section 31A-2-403;

(b) the County Recorder Standards Board created in Section 63C-30-201; and

(c) other relevant industry stakeholders.

Section 6. Section **63A-16-104** is amended to read:

63A-16-104 . Duties of division.

The division shall:

(1) lead state executive branch agency efforts to establish and reengineer the state's information technology architecture with the goal of coordinating central and individual agency information technology in a manner that:

(a) ensures compliance with the executive branch agency strategic plan; and

(b) ensures that cost-effective, efficient information and communication systems and resources are being used by agencies to:

(i) reduce data, hardware, and software redundancy;

(ii) improve system interoperability and data accessibility between agencies; and

(iii) meet the agency's and user's business and service needs;

(2) coordinate an executive branch strategic plan for all agencies;

(3) develop and implement processes to replicate information technology best practices and standards throughout the executive branch;

(4) once every three years:

(a) conduct an information technology security assessment via an independent third party:

(i) to evaluate the adequacy of the division's and the executive branch agencies' data and information technology system security standards; and

(ii) that will be completed over a period that does not exceed two years; and

(b) communicate the results of the assessment described in Subsection (4)(a) to the appropriate executive branch agencies and to the president of the Senate and the speaker of the House of Representatives;

(5) subject to Subsection 63G-6a-109.5(9):

(a) advise executive branch agencies on project and contract management principles as they relate to information technology projects within the executive branch; and

(b) approve the acquisition of technology services and products by executive branch agencies as required under Section 63G-6a-109.5;

(6) work toward building stronger partnering relationships with providers;

(7) develop service level agreements with executive branch departments and agencies to ensure quality products and services are delivered on schedule and within budget;

(8) develop standards for application development including a standard methodology and cost-benefit analysis that all agencies shall utilize for application development activities;

(9) determine and implement statewide efforts to standardize data elements;

(10) coordinate with executive branch agencies to provide basic website standards for agencies that address common design standards and navigation standards, including:

(a) accessibility for individuals with disabilities in accordance with:

(i) the standards of 29 U.S.C. Sec. 794d; and

(ii) Section 63A-16-209;

(b) consistency with standardized government security standards;

(c) designing around user needs with data-driven analysis influencing management and development decisions, using qualitative and quantitative data to determine user goals, needs, and behaviors, and continual testing of the website, web-based form, web-based application, or digital service to ensure that user needs are addressed;

(d) providing users of the website, web-based form, web-based application, or digital service with the option for a more customized digital experience that allows users to complete digital transactions in an efficient and accurate manner; and

(e) full functionality and usability on common mobile devices;

(11) consider, when making a purchase for an information system, cloud computing options, including any security benefits, privacy, data retention risks, and cost savings associated with cloud computing options;

(12) develop systems and methodologies to review, evaluate, and prioritize existing information technology projects within the executive branch and report to the governor and the Government Operations Interim Committee in accordance with Section 63A-16-201 on a semiannual basis regarding the status of information technology projects;

(13) assist the Governor's Office of Planning and Budget with the development of information technology budgets for agencies;

(14) ensure that any training or certification required of a public official or public employee, as those terms are defined in Section 63G-22-102, complies with Title 63G, Chapter 22, State Training and Certification Requirements, if the training or certification is required:

(a) under this chapter;

(b) by the department; or

(c) by the division;

(15) provide support to executive branch agencies for the information technology assets and functions that are unique to the agency and are mission critical functions of the agency;

(16) provide in-house information technology staff support to executive branch agencies;

(17) establish a committee composed of agency user groups to coordinate division services with agency needs;

(18) assist executive branch agencies in complying with the requirements of any rule made by the chief information officer;

(19) develop and implement an effective enterprise architecture governance model for the executive branch;

(20) provide oversight of information technology projects that impact statewide information technology services, assets, or functions of state government to:

(a) control costs;

(b) ensure business value to a project;

(c) maximize resources;

(d) ensure the uniform application of best practices; and

(e) avoid duplication of resources;

(21) develop a method of accountability to agencies for services provided by the

department through service agreements with the agencies;

(22) serve as a project manager for enterprise architecture, including management of applications, standards, and procurement of enterprise architecture;

(23) coordinate the development and implementation of advanced state telecommunication systems;

(24) provide services, including technical assistance:

(a) to executive branch agencies and subscribers to the services; and

(b) related to information technology or telecommunications;

(25) establish telecommunication system specifications and standards for use by:

(a) one or more executive branch agencies; or

(b) one or more entities that subscribe to the telecommunication systems in accordance with Section 63A-16-302;

(26) coordinate state telecommunication planning, in cooperation with:

(a) state telecommunication users;

(b) executive branch agencies; and

(c) other subscribers to the state's telecommunication systems;

(27) cooperate with the federal government, other state entities, counties, and municipalities in the development, implementation, and maintenance of:

(a)(i) governmental information technology; or

(ii) governmental telecommunication systems; and

(b)(i) as part of a cooperative organization; or

(ii) through means other than a cooperative organization;

(28) establish, operate, manage, and maintain:

(a) one or more state data centers; and

(b) one or more regional computer centers;

(29) design, implement, and manage all state-owned, leased, or rented land, mobile, or radio telecommunication systems that are used in the delivery of services for state government or the state's political subdivisions;

(30) in accordance with the executive branch strategic plan, implement minimum standards to be used by the division for purposes of compatibility of procedures, programming languages, codes, and media that facilitate the exchange of information within and among telecommunication systems;

(31) establish standards for the information technology needs of a collection of executive branch agencies or programs that share common characteristics relative to the types of

stakeholders the agencies or programs serve, including:

(a) project management;

(b) application development; and

(c) subject to Subsections (5) and 63G-6a-109.5(9), procurement;

(32) provide oversight of information technology standards that impact multiple executive branch agency information technology services, assets, or functions to:

(a) control costs;

(b) ensure business value to a project;

(c) maximize resources;

(d) ensure the uniform application of best practices; and

(e) avoid duplication of resources;

(33) establish a system of accountability to user agencies through the use of service agreements;[~~and~~]

(34) provide the services described in Section 63A-16-109 for a state elected official or state employee who has been threatened[~~.~~] ; and

(35) provide technical consultation to the State Archives regarding digital authentication systems in accordance with Section 63A-16-215.

Section 7. Section **63A-16-215** is enacted to read:

63A-16-215 . Digital authentication system technical support.

(1) As used in this section:

(a) "Digital authentication system" means technology and procedures used to create digitally authenticated records.

(b) "Digitally authenticated record" means the same as that term is defined in Section 17-71-301.5.

(c) "Governmental entity" means the same as that term is defined in Section 63G-2-103.

(d) "State Archives" means the Division of Archives and Records Service created in Section 63A-12-101.

(2) The division shall provide technical consultation to the State Archives regarding:

(a) security standards for digital authentication systems;

(b) cybersecurity requirements;

(c) authentication technologies and methods; and

(d) system integrity standards.

(3) The division may provide technical assistance to governmental entities implementing digital authentication systems approved under Section 17-71-301.5.

Section 8. **Effective Date.**

This bill takes effect on May 6, 2026.