

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 as an alternative to traditionally notarized documents;
  - establishes requirements for digital authentication standards;
  - requires review and approval from the State Archives before county implementation;
  - provides that digitally authenticated records have the same legal effect as notarized documents when requirements are met;
  - 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:

- 29 **17-71-301**, as renumbered and amended by Laws of Utah 2025, First Special Session,
- 30 Chapter 13
- 31 **46-1-2**, as last amended by Laws of Utah 2025, First Special Session, Chapter 16
- 32 **57-3-101**, as last amended by Laws of Utah 2025, First Special Session, Chapter 15
- 33 **63A-12-101**, as last amended by Laws of Utah 2025, Chapter 476
- 34 **63A-12-104**, as last amended by Laws of Utah 2025, Chapter 475
- 35 **63A-16-104**, as last amended by Laws of Utah 2024, Chapter 508

36 ENACTS:

- 37 **17-71-301.5**, Utah Code Annotated 1953
- 38 **57-3-101.5**, Utah Code Annotated 1953
- 39 **63A-12-117**, Utah Code Annotated 1953
- 40 **63A-16-215**, Utah Code Annotated 1953

41 

---

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

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

44 **17-71-301 . Document custody responsibility -- Compliance with County**  
 45 **Recorder Standards Board rules -- Compliance with county appeal authority.**

46 The county recorder:

- 47 (1) is custodian of all recorded documents, records, and associated data required by law to
- 48 be recorded;
- 49 (2) shall comply with rules made by the County Recorder Standards Board under Section
- 50 63C-30-202, including rules that govern:
  - 51 (a) the protection of recorded documents and records in the county recorder's custody;
  - 52 (b) the electronic submission of plats, records, and other documents to the county
  - 53 recorder's office;
  - 54 (c) the protection of privacy interests in the case of documents and records in the county
  - 55 recorder's custody; and
  - 56 (d) the formatting, recording, and redaction of documents and records in the county
  - 57 recorder's custody;
- 58 (3) shall comply with the appeal authority established by the county legislative body in
- 59 accordance with Section 17-71-306; ~~and~~
- 60 (4) may adopt policies and procedures governing the office of the county recorder that do
- 61 not conflict with this chapter or rules made by the County Recorder Standards Board
- 62 under Section 63C-30-202[-] ; and

63 (5) shall comply with approval requirements described in Section 17-71-301.5 before  
64 accepting digitally authenticated records as defined in Section 46-1-2.

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

66 **17-71-301.5 . Digital authentication of county records -- Standards and approval**  
67 **process.**

68 (1) As used in this section:

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

71 (b) "Digitally authenticated record" means the same as that term is defined in Section  
72 46-1-2.

73 (c) "Division" means the Division of Technology Services created in Section  
74 63A-16-103.

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

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

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

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

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

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

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

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

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

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

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

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

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

92 (ii) security measures to protect record integrity;

93 (iii) procedures for verification of authentication;

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

95 (v) implementation timelines and training plans;

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

- 97                    Committee;
- 98                    (vii) preservation requirements for permanent records;
- 99                    (viii) transfer procedures for records to be archived;
- 100                   (ix) format specifications for long-term storage;
- 101                   (x) consultation conducted with:
- 102                    (A) the Title and Escrow Commission created in Section 31A-2-403;
- 103                    (B) the County Recorder Standards Board created in Section 63C-30-201; and
- 104                    (C) other private industry stakeholders with interests affected by the proposal; and
- 105                   (xi) a summary of concerns raised during the consultations described in Subsection
- 106                    (3)(a)(x); and
- 107                   (b) obtain approval from the state archivist in accordance with Subsection (4).
- 108                   (4)(a) The state archivist shall review each county proposal submitted under Subsection
- 109                   (3) for:
- 110                    (i) compliance with:
- 111                    (A) retention schedules approved by the Records Management Committee;
- 112                    (B) preservation standards for digital records established under Section
- 113                    63A-12-117;
- 114                    (C) transfer requirements for permanent records; and
- 115                    (D) technical standards established by rule under Section 63A-12-117;
- 116                   (ii) sufficiency of county resources and training for implementation; and
- 117                   (iii) completeness of the consultation requirements described in Subsection (3)(a)(x)
- 118                    and consideration of concerns described in Subsection (3)(a)(xi).
- 119                   (b) The state archivist shall consult with the division regarding technical aspects of a
- 120                    proposal.
- 121                   (c) Before the state archivist approves a proposal, the county, with assistance from State
- 122                    Archives, shall present the proposal to the Records Management Committee in a
- 123                    public meeting that provides opportunity for public comment.
- 124                   (d) The state archivist shall provide written approval or denial to the county within 45
- 125                    days after the day on which the county submits a proposal under Subsection (3).
- 126                   (e) If the state archivist denies a proposal, the state archivist shall provide:
- 127                    (i) specific reasons for denial; and
- 128                    (ii) recommendations for modification.
- 129                   (f) A county may resubmit a modified proposal in accordance with this section.
- 130                   (5) An approval granted under Subsection (4) is valid for three years and may be renewed

131 upon demonstration of continued compliance with the requirements of this section.

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

134 Section 3. Section **46-1-2** is amended to read:

135 **46-1-2 . Definitions.**

136 As used in this chapter:

137 (1) "Acknowledgment" means a notarial act in which a notary certifies that a signer, whose  
 138 identity is personally known to the notary or proven on the basis of satisfactory  
 139 evidence, has admitted, in the presence of the notary, to voluntarily signing a document  
 140 for the document's stated purpose.

141 (2) "Before me" means that an individual appears in the presence of the notary.

142 (3) "Commission" means:

143 (a) to empower to perform notarial acts; or

144 (b) the written document that gives authority to perform notarial acts, including the  
 145 Certificate of Authority of Notary Public that the lieutenant governor issues to a  
 146 notary.

147 (4) "Copy certification" means a notarial act in which a notary certifies that a photocopy is  
 148 an accurate copy of a document that is neither a public record nor publicly recorded.

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

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

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

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

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

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

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

158 [~~5~~] (7) "Electronic notarization" means:

159 (a) a remote notarization; or

160 (b) a notarization:

161 (i) in an electronic format;

162 (ii) of a document that may be recorded electronically under Subsection 17-71-402(2);

163 and

164 (iii) that conforms with rules made under Section 46-1-3.7.

- 165 [(6)] (8) "Electronic recording" means the audio and video recording, described in  
166 Subsection 46-1-3.6(3), of a remote notarization.
- 167 [(7)] (9) "Electronic seal" means an electronic version of the seal described in Section  
168 46-1-16, that conforms with rules made under Subsection 46-1-3.7(1)(d), that a notary  
169 may attach to a notarial certificate to complete an electronic notarization.
- 170 [(8)] (10) "Electronic signature" means the same as that term is defined in Section 46-4-102.
- 171 [(9)] (11) "In the presence of the notary" means that an individual:
- 172 (a) is physically present with the notary in close enough proximity to see and hear the  
173 notary; or
- 174 (b) communicates with a remote notary by means of an electronic device or process that:
- 175 (i) allows the individual and remote notary to communicate with one another  
176 simultaneously by sight and sound; and
- 177 (ii) complies with rules made under Section 46-1-3.7.
- 178 [(10)] (12) "Jurat" means a notarial act in which a notary certifies:
- 179 (a) the identity of a signer who:
- 180 (i) is personally known to the notary; or
- 181 (ii) provides the notary satisfactory evidence of the signer's identity;
- 182 (b) that the signer affirms or swears an oath attesting to the truthfulness of a document;  
183 and
- 184 (c) that the signer voluntarily signs the document in the presence of the notary.
- 185 [(11)] (13) "Notarial act" or "notarization" means an act that a notary is authorized to  
186 perform under Section 46-1-6.
- 187 [(12)] (14) "Notarial certificate" means the affidavit described in Section 46-1-6.5 that is:
- 188 (a) a part of or attached to a notarized document; and
- 189 (b) completed by the notary and bears the notary's signature and official seal.
- 190 [(13)] (15)(a) "Notary" means an individual commissioned to perform notarial acts under  
191 this chapter.
- 192 (b) "Notary" includes a remote notary.
- 193 [(14)] (16) "Oath" or "affirmation" means a notarial act in which a notary certifies that a  
194 person made a vow or affirmation in the presence of the notary on penalty of perjury.
- 195 [(15)] (17) "Official misconduct" means a notary's performance of any act prohibited or  
196 failure to perform any act mandated by this chapter or by any other law in connection  
197 with a notarial act.
- 198 [(16)] (18)(a) "Official seal" means the seal described in Section 46-1-16 that a notary

- 199 may attach to a notarial certificate to complete a notarization.
- 200 (b) "Official seal" includes an electronic seal.
- 201 [(17)] (19) "Personally known" means familiarity with an individual resulting from  
202 interactions with that individual over a period of time sufficient to eliminate every  
203 reasonable doubt that the individual has the identity claimed.
- 204 [(18)] (20) "Remote notarization" means a notarial act performed by a remote notary in  
205 accordance with this chapter for an individual who is not in the physical presence of the  
206 remote notary at the time the remote notary performs the notarial act.
- 207 [(19)] (21) "Remote notary" means a notary that holds an active remote notary certification  
208 under Section 46-1-3.5.
- 209 [(20)] (22)(a) "Satisfactory evidence of identity" means:
- 210 (i) for both an in-person and remote notarization, identification of an individual based  
211 on:
- 212 (A) subject to Subsection [(20)(b)] (22)(b), valid personal identification with the  
213 individual's photograph, signature, and physical description that the United  
214 States government, any state within the United States, or a foreign government  
215 issues;
- 216 (B) subject to Subsection [(20)(b)] (22)(b), a valid passport that any nation issues;  
217 or
- 218 (C) the oath or affirmation of a credible person who is personally known to the  
219 notary and who personally knows the individual; and
- 220 (ii) for a remote notarization only, a third party's affirmation of an individual's  
221 identity in accordance with rules made under Section 46-1-3.7 by means of:
- 222 (A) dynamic knowledge-based authentication, which may include requiring the  
223 individual to answer questions about the individual's personal information  
224 obtained from public or proprietary data sources; or
- 225 (B) analysis of the individual's biometric data, which may include facial  
226 recognition, voiceprint analysis, or fingerprint analysis.
- 227 (b) "Satisfactory evidence of identity," for a remote notarization, requires the  
228 identification described in Subsection [(20)(a)(i)(A)] (22)(a)(i)(A) or passport  
229 described in Subsection [(20)(a)(i)(B)] (22)(a)(i)(B) to be verified through public or  
230 proprietary data sources in accordance with rules made under Section 46-1-3.7.
- 231 (c) "Satisfactory evidence of identity" does not include:
- 232 (i) a driving privilege card under Subsection 53-3-207(12); or

233 (ii) another document that is not considered valid for identification.

234 [(21)] (23) "Signature witnessing" means a notarial act in which an individual:

- 235 (a) appears in the presence of the notary and presents a document;
- 236 (b) provides the notary satisfactory evidence of the individual's identity, or is personally
- 237 known to the notary; and
- 238 (c) signs the document in the presence of the notary.

239 (24) "Tamper-evident technology" means technology that:

- 240 (a) creates a permanent, verifiable record that allows detection of any unauthorized
- 241 alteration to an electronic document after authentication; and
- 242 (b) maintains an immutable audit trail of authentication events.

243 Section 4. Section **57-3-101** is amended to read:

244 **57-3-101 . Certificate of acknowledgment, proof of execution, jurat, or other**  
245 **certificate required -- Notarial acts affecting real property -- Right to record documents**  
246 **unaffected by subdivision ordinances.**

247 (1) A certificate of the acknowledgment of any document, or of the proof of the execution  
248 of any document, or a jurat as defined in Section 46-1-2, or other notarial certificate  
249 containing the words "subscribed and sworn" or their substantial equivalent, that is  
250 signed and certified by the officer taking the acknowledgment, proof, or jurat, as  
251 provided in this title, or a digitally authenticated record as provided in Section  
252 57-3-101.5, entitles the document and the certificate to be recorded in the office of the  
253 recorder of the county where the real property is located.

254 (2) Notarial acts affecting real property in this state shall also be performed in conformance  
255 with Title 46, Chapter 1, Notaries Public Reform Act.

256 (3) Nothing in the provisions of Title 10, Chapter 20, Part 8, Subdivisions, and Title 17,  
257 Chapter 79, Part 7, Subdivisions, shall prohibit the recording of a document which is  
258 otherwise entitled to be recorded under the provisions of this chapter.

259 Section 5. Section **57-3-101.5** is enacted to read:

260 **57-3-101.5 . Digital authentication as alternative to notarization.**

261 (1) As used in this section:

- 262 (a) "Digital authentication" means the same as that term is defined in Section 46-1-2.
- 263 (b) "Digitally authenticated record" means the same as that term is defined in Section
- 264 46-1-2.

265 (2) A digitally authenticated record has the same legal effect for recording purposes as a  
266 document that contains a certificate of acknowledgment, proof of execution, jurat, or

267 other certificate described in Section 57-3-101 if:

268 (a) the digitally authenticated record meets the standards established by the state

268a archivist

269 under Section 63A-12-117; and

270 (b) if the digitally authenticated record is to be recorded by a county recorder, the county

271 has obtained approval under Section 17-71-301.5.

272 (3) This section does not:

273 (a) require a person to use digital authentication;

274 (b) invalidate a document authenticated by traditional notarization under Section

275 57-3-101; or

276 (c) require a county recorder to accept digitally authenticated records.

277 Section 6. Section **63A-12-101** is amended to read:

278 **63A-12-101 . Division of Archives and Records Service created -- Duties.**

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

280 (2) The state archives shall:

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

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

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

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

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

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

297 (g) provide staff and support services to the Records Management Committee created in  
298 Section 63A-12-112 and the Government Records Office, created in Section  
299 63A-12-202;

- 300 (h) develop training programs to assist records officers and other interested officers and  
 301 employees of governmental entities to administer this chapter and Title 63G, Chapter  
 302 2, Government Records Access and Management Act;
- 303 (i) provide access to public records deposited in the archives;
- 304 (j) administer and maintain the Utah Public Notice Website established under Section  
 305 63A-16-601;
- 306 (k) provide assistance to any governmental entity in administering this chapter and Title  
 307 63G, Chapter 2, Government Records Access and Management Act;
- 308 (l) prepare forms for use by all governmental entities for a person requesting access to a  
 309 record; [~~and~~]
- 310 (m) if the department operates the Division of Archives and Records Service as an  
 311 internal service fund agency in accordance with Section 63A-1-109.5, submit to the  
 312 Rate Committee established in Section 63A-1-114:
- 313 (i) the proposed rate schedule as required by Section 63A-1-114; and  
 314 (ii) other information or analysis requested by the Rate Committee[-] ; and
- 315 (n) establish standards for digital authentication systems and review county proposals  
 316 for accepting digitally authenticated records in accordance with Section 17-71-301.5.
- 317 (3) The state archives may:
- 318 (a) establish a report and directives management program;
- 319 (b) establish a forms management program; and
- 320 (c) in accordance with Section 63A-12-101, require that an individual undergo a  
 321 background check if the individual:
- 322 (i) applies to be, or currently is, an employee or volunteer of the division; and  
 323 (ii) will have direct access to a vulnerable record in the capacity described in  
 324 Subsection (3)(c)(i).
- 325 (4) The executive director may direct the state archives to administer other functions or  
 326 services consistent with this chapter and Title 63G, Chapter 2, Government Records  
 327 Access and Management Act.
- 328 Section 7. Section **63A-12-104** is amended to read:
- 329 **63A-12-104 . Rulemaking authority.**
- 330 In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act:
- 331 (1) the state archivist may make rules establishing:
- 332 (a) procedures for the collection, storage, designation, classification, access, mediation  
 333 for records access, and management of records under this chapter and Title 63G,

334 Chapter 2, Government Records Access and Management Act; and  
 335 (b) procedures and standards for digital authentication systems and preservation of  
 336 digitally authenticated records in accordance with Section 63A-12-117; and  
 337 (2) a governmental entity may make rules, policies, or ordinances specifying at which level  
 338 within the governmental entity the requirements described in this chapter will be  
 339 undertaken.

340 Section 8. Section **63A-12-117** is enacted to read:

341 **63A-12-117 . Digital authentication systems -- Technical standards and**  
 342 **requirements.**

343 (1) As used in this section:

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

346 (b) "Digitally authenticated record" means the same as that term is defined in Section  
 347 46-1-2.

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

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

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

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

352 (c) Ĥ→ **except as otherwise prohibited by law,** ←Ĥ transfer records to the state archives  
 352a in accordance with state archivist requirements;

353 and

354 (d) maintain data necessary for verification and preservation.

355 (3) The state archivist shall establish procedures for:

356 (a) accepting digitally authenticated permanent records;

357 (b) verifying authentication integrity upon transfer;

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

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

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

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

365 (A) security requirements;

366 (B) authentication verification procedures;

- 367           (C) acceptable authentication methods and technologies;  
 368           (D) cybersecurity standards; and  
 369           (E) system integrity requirements;  
 370       (ii) preservation standards for digital authentication systems to ensure long-term  
 371           preservation;  
 372       (iii) retention schedule requirements for digitally authenticated records;  
 373       (iv) transfer procedures from governmental entities to state archives;  
 374       (v) format specifications for archival storage of digitally authenticated records;  
 375       (vi) verification procedures for authentication integrity; and  
 376       (vii) data requirements for preservation and access.  
 377       (b) The state archivist shall ensure that standards established under this section require  
 378           digitally authenticated records to demonstrate:  
 379           (i) immutability or tamper-evident characteristics sufficient to detect unauthorized  
 380               alterations;  
 381           (ii) verified identity of the person authenticating the record using identity verification  
 382               procedures that meet or exceed the requirements for satisfactory evidence of  
 383               identity established for notarization under Section 46-1-2;  
 384           (iii) format sustainability for long-term preservation; and  
 385           (iv) compliance with retention schedules.  
 386       (5) In making rules under Subsection (4), the state archivist shall consult with:  
 387           (a) the Title and Escrow Commission created in Section 31A-2-403;  
 388           (b) the County Recorder Standards Board created in Section 63C-30-201; and  
 389           (c) other relevant industry stakeholders.

390       Section 9. Section **63A-16-104** is amended to read:

391       **63A-16-104 . Duties of division.**

392       The division shall:

- 393       (1) lead state executive branch agency efforts to establish and reengineer the state's  
 394       information technology architecture with the goal of coordinating central and individual  
 395       agency information technology in a manner that:  
 396       (a) ensures compliance with the executive branch agency strategic plan; and  
 397       (b) ensures that cost-effective, efficient information and communication systems and  
 398       resources are being used by agencies to:  
 399           (i) reduce data, hardware, and software redundancy;  
 400           (ii) improve system interoperability and data accessibility between agencies; and

- 401 (iii) meet the agency's and user's business and service needs;
- 402 (2) coordinate an executive branch strategic plan for all agencies;
- 403 (3) develop and implement processes to replicate information technology best practices and  
404 standards throughout the executive branch;
- 405 (4) once every three years:
- 406 (a) conduct an information technology security assessment via an independent third  
407 party:
- 408 (i) to evaluate the adequacy of the division's and the executive branch agencies' data  
409 and information technology system security standards; and
- 410 (ii) that will be completed over a period that does not exceed two years; and
- 411 (b) communicate the results of the assessment described in Subsection (4)(a) to the  
412 appropriate executive branch agencies and to the president of the Senate and the  
413 speaker of the House of Representatives;
- 414 (5) subject to Subsection 63G-6a-109.5(9):
- 415 (a) advise executive branch agencies on project and contract management principles as  
416 they relate to information technology projects within the executive branch; and
- 417 (b) approve the acquisition of technology services and products by executive branch  
418 agencies as required under Section 63G-6a-109.5;
- 419 (6) work toward building stronger partnering relationships with providers;
- 420 (7) develop service level agreements with executive branch departments and agencies to  
421 ensure quality products and services are delivered on schedule and within budget;
- 422 (8) develop standards for application development including a standard methodology and  
423 cost-benefit analysis that all agencies shall utilize for application development activities;
- 424 (9) determine and implement statewide efforts to standardize data elements;
- 425 (10) coordinate with executive branch agencies to provide basic website standards for  
426 agencies that address common design standards and navigation standards, including:
- 427 (a) accessibility for individuals with disabilities in accordance with:
- 428 (i) the standards of 29 U.S.C. Sec. 794d; and
- 429 (ii) Section 63A-16-209;
- 430 (b) consistency with standardized government security standards;
- 431 (c) designing around user needs with data-driven analysis influencing management and  
432 development decisions, using qualitative and quantitative data to determine user  
433 goals, needs, and behaviors, and continual testing of the website, web-based form,  
434 web-based application, or digital service to ensure that user needs are addressed;

- 435 (d) providing users of the website, web-based form, web-based application, or digital  
436 service with the option for a more customized digital experience that allows users to  
437 complete digital transactions in an efficient and accurate manner; and
- 438 (e) full functionality and usability on common mobile devices;
- 439 (11) consider, when making a purchase for an information system, cloud computing  
440 options, including any security benefits, privacy, data retention risks, and cost savings  
441 associated with cloud computing options;
- 442 (12) develop systems and methodologies to review, evaluate, and prioritize existing  
443 information technology projects within the executive branch and report to the governor  
444 and the Government Operations Interim Committee in accordance with Section  
445 63A-16-201 on a semiannual basis regarding the status of information technology  
446 projects;
- 447 (13) assist the Governor's Office of Planning and Budget with the development of  
448 information technology budgets for agencies;
- 449 (14) ensure that any training or certification required of a public official or public  
450 employee, as those terms are defined in Section 63G-22-102, complies with Title 63G,  
451 Chapter 22, State Training and Certification Requirements, if the training or certification  
452 is required:
- 453 (a) under this chapter;
- 454 (b) by the department; or
- 455 (c) by the division;
- 456 (15) provide support to executive branch agencies for the information technology assets and  
457 functions that are unique to the agency and are mission critical functions of the agency;
- 458 (16) provide in-house information technology staff support to executive branch agencies;
- 459 (17) establish a committee composed of agency user groups to coordinate division services  
460 with agency needs;
- 461 (18) assist executive branch agencies in complying with the requirements of any rule made  
462 by the chief information officer;
- 463 (19) develop and implement an effective enterprise architecture governance model for the  
464 executive branch;
- 465 (20) provide oversight of information technology projects that impact statewide information  
466 technology services, assets, or functions of state government to:
- 467 (a) control costs;
- 468 (b) ensure business value to a project;

- 469 (c) maximize resources;
- 470 (d) ensure the uniform application of best practices; and
- 471 (e) avoid duplication of resources;
- 472 (21) develop a method of accountability to agencies for services provided by the
- 473 department through service agreements with the agencies;
- 474 (22) serve as a project manager for enterprise architecture, including management of
- 475 applications, standards, and procurement of enterprise architecture;
- 476 (23) coordinate the development and implementation of advanced state telecommunication
- 477 systems;
- 478 (24) provide services, including technical assistance:
- 479 (a) to executive branch agencies and subscribers to the services; and
- 480 (b) related to information technology or telecommunications;
- 481 (25) establish telecommunication system specifications and standards for use by:
- 482 (a) one or more executive branch agencies; or
- 483 (b) one or more entities that subscribe to the telecommunication systems in accordance
- 484 with Section 63A-16-302;
- 485 (26) coordinate state telecommunication planning, in cooperation with:
- 486 (a) state telecommunication users;
- 487 (b) executive branch agencies; and
- 488 (c) other subscribers to the state's telecommunication systems;
- 489 (27) cooperate with the federal government, other state entities, counties, and municipalities
- 490 in the development, implementation, and maintenance of:
- 491 (a)(i) governmental information technology; or
- 492 (ii) governmental telecommunication systems; and
- 493 (b)(i) as part of a cooperative organization; or
- 494 (ii) through means other than a cooperative organization;
- 495 (28) establish, operate, manage, and maintain:
- 496 (a) one or more state data centers; and
- 497 (b) one or more regional computer centers;
- 498 (29) design, implement, and manage all state-owned, leased, or rented land, mobile, or
- 499 radio telecommunication systems that are used in the delivery of services for state
- 500 government or the state's political subdivisions;
- 501 (30) in accordance with the executive branch strategic plan, implement minimum standards
- 502 to be used by the division for purposes of compatibility of procedures, programming

- 503 languages, codes, and media that facilitate the exchange of information within and  
504 among telecommunication systems;
- 505 (31) establish standards for the information technology needs of a collection of executive  
506 branch agencies or programs that share common characteristics relative to the types of  
507 stakeholders the agencies or programs serve, including:
- 508 (a) project management;  
509 (b) application development; and  
510 (c) subject to Subsections (5) and 63G-6a-109.5(9), procurement;
- 511 (32) provide oversight of information technology standards that impact multiple executive  
512 branch agency information technology services, assets, or functions to:
- 513 (a) control costs;  
514 (b) ensure business value to a project;  
515 (c) maximize resources;  
516 (d) ensure the uniform application of best practices; and  
517 (e) avoid duplication of resources;
- 518 (33) establish a system of accountability to user agencies through the use of service  
519 agreements; [and]
- 520 (34) provide the services described in Section 63A-16-109 for a state elected official or  
521 state employee who has been threatened[-] ; and
- 522 (35) provide technical consultation to the State Archives regarding digital authentication  
523 systems in accordance with Section 63A-16-215.

524 Section 10. Section **63A-16-215** is enacted to read:

525 **63A-16-215 . Digital authentication system technical support.**

- 526 (1) As used in this section:
- 527 (a) "Digital authentication system" means technology and procedures used to create  
528 digitally authenticated records.
- 529 (b) "Digitally authenticated record" means the same as that term is defined in Section  
530 46-1-2.
- 531 (c) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
- 532 (d) "State Archives" means the Division of Archives and Records Service created in  
533 Section 63A-12-101.
- 534 (2) The division shall provide technical consultation to the State Archives regarding:
- 535 (a) security standards for digital authentication systems;  
536 (b) cybersecurity requirements;

537 (c) authentication technologies and methods; and

538 (d) system integrity standards.

539 (3) The division may provide technical assistance to governmental entities implementing

540 digital authentication systems approved under Section 17-71-301.5.

541 Section 11. **Effective Date.**

542 This bill takes effect on May 6, 2026.