

1

Electronic Records Amendments

2026 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Paul A. Cutler

Senate Sponsor: Wayne A. Harper

2

LONG TITLE

3

General Description:

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

7

Highlighted Provisions:

8

This bill:

9

- ▶ defines terms;

10

- ▶ authorizes counties to accept digitally authenticated records as an alternative to
11 traditionally notarized documents;

12

- ▶ establishes requirements for digital authentication standards;

13

- ▶ requires review and approval from the State Archives before county implementation;

14

- ▶ provides that digitally authenticated records have the same legal effect as notarized
15 documents when requirements are met;

16

- ▶ requires the State Archivist to establish retention and preservation standards for digital
17 records;

18

- ▶ grants rulemaking authority to the State Archivist in consultation with the Division of
19 Technology Services;

20

- ▶ requires approval processes for counties before accepting digitally authenticated records;
21 and

22

- ▶ makes technical and conforming changes.

23

Money Appropriated in this Bill:

24

None

25

Other Special Clauses:

26

None

27

Utah Code Sections Affected:

28

AMENDS:

29

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

31 **17-71-602**, as renumbered and amended by Laws of Utah 2025, First Special Session,
32 Chapter 13
33 **46-1-2**, as last amended by Laws of Utah 2025, First Special Session, Chapter 16
34 **57-3-101**, as last amended by Laws of Utah 2025, First Special Session, Chapter 15
35 **63A-12-101**, as last amended by Laws of Utah 2025, Chapter 476
36 **63A-12-104**, as last amended by Laws of Utah 2025, Chapter 475
37 **63A-16-104**, as last amended by Laws of Utah 2024, Chapter 508

38 ENACTS:

39 **17-71-301.5**, Utah Code Annotated 1953
40 **57-3-101.5**, Utah Code Annotated 1953
41 **63A-12-117**, Utah Code Annotated 1953
42 **63A-16-215**, Utah Code Annotated 1953

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

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

46 **17-71-301 . Document custody responsibility -- Compliance with County
47 Recorder Standards Board rules -- Compliance with county appeal authority.**

48 The county recorder:

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

51 (2) shall comply with rules made by the County Recorder Standards Board under Section
52 63C-30-202, including rules that govern:
53 (a) the protection of recorded documents and records in the county recorder's custody;
54 (b) the electronic submission of plats, records, and other documents to the county
55 recorder's office;
56 (c) the protection of privacy interests in the case of documents and records in the county
57 recorder's custody; and
58 (d) the formatting, recording, and redaction of documents and records in the county
59 recorder's custody;

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

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

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

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

68 **17-71-301.5 . Digital authentication of county records -- Standards and approval**
69 **process.**

70 (1) As used in this section:

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

73 (b) "Digitally authenticated record" means the same as that term is defined in Section
74 46-1-2.

75 (c) "Division" means the Division of Technology Services created in Section
76 63A-16-103.

77 (d) "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; and

100 (ix) format specifications for long-term storage; and

101 (b) obtain approval from the State Archivist in accordance with Subsection (4).

102 (4)(a) The State Archivist shall review each county proposal submitted under Subsection

103 (3) for compliance with:

104 (i) retention schedules approved by the Records Management Committee;

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

106 (iii) transfer requirements for permanent records;

107 (iv) technical standards established by rule under Section 63A-12-117; and

108 (v) adequacy of county resources and training for implementation.

109 (b) The State Archivist shall consult with the division regarding technical aspects of a
110 proposal.

111 (c) The State Archivist shall provide written approval or denial to the county within 45
112 days after the day on which the county submits a proposal under Subsection (3).

113 (d) If the State Archivist denies a proposal, the State Archivist shall provide:

114 (i) specific reasons for denial; and

115 (ii) recommendations for modification.

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

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

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

121 Section 3. Section **17-71-602** is amended to read:

122 **17-71-602 . Validity of electronic documents.**

123 (1) If a law requires, as a condition for recording, that a document be an original, be on
124 paper or another tangible medium, or be in writing, the requirement is satisfied by an
125 electronic document satisfying this chapter.

126 (2) If a law requires, as a condition for recording, that a document be signed, the
127 requirement is satisfied by an electronic signature.

128 (3)(a) A requirement that a document or a signature associated with a document be
129 notarized, acknowledged, verified, witnessed, or made under oath is satisfied if:

130 (i) the electronic signature of the person authorized to perform that act, and all other
131 information required to be included, is attached to or logically associated with the
132 document or signature[.] ; or

(ii) the document is a digitally authenticated record that meets the requirements established under Section 17-71-301.5.

(b) A physical or electronic image of a stamp, impression, or seal need not accompany an electronic signature.

Section 4. Section **46-1-2** is amended to read:

46-1-2 . Definitions.

As used in this chapter:

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

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

(3) "Commission" means:

(a) to empower to perform notarial acts; or

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

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

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

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

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

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

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

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

(c) 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.

[**(5)**] (7) "Electronic notarization" means:

(a) a remote notarization; or

(b) a notarization:

(i) in an electronic format;

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

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

168 [6] (8) "Electronic recording" means the audio and video recording, described in
169 Subsection 46-1-3.6(3), of a remote notarization.

170 [7] (9) "Electronic seal" means an electronic version of the seal described in Section
171 46-1-16, that conforms with rules made under Subsection 46-1-3.7(1)(d), that a notary
172 may attach to a notarial certificate to complete an electronic notarization.

173 [8] (10) "Electronic signature" means the same as that term is defined in Section 46-4-102.

174 [9] (11) "In the presence of the notary" means that an individual:

- 175 (a) is physically present with the notary in close enough proximity to see and hear the
176 notary; or
- 177 (b) communicates with a remote notary by means of an electronic device or process that:
 - 178 (i) allows the individual and remote notary to communicate with one another
179 simultaneously by sight and sound; and
 - 180 (ii) complies with rules made under Section 46-1-3.7.

181 [10] (12) "Jurat" means a notarial act in which a notary certifies:

- 182 (a) the identity of a signer who:
 - 183 (i) is personally known to the notary; or
 - 184 (ii) provides the notary satisfactory evidence of the signer's identity;
- 185 (b) that the signer affirms or swears an oath attesting to the truthfulness of a document;
186 and
- 187 (c) that the signer voluntarily signs the document in the presence of the notary.

188 [11] (13) "Notarial act" or "notarization" means an act that a notary is authorized to
189 perform under Section 46-1-6.

190 [12] (14) "Notarial certificate" means the affidavit described in Section 46-1-6.5 that is:
191 (a) a part of or attached to a notarized document; and
192 (b) completed by the notary and bears the notary's signature and official seal.

193 [13] (15)(a) "Notary" means an individual commissioned to perform notarial acts under
194 this chapter.
195 (b) "Notary" includes a remote notary.

196 [14] (16) "Oath" or "affirmation" means a notarial act in which a notary certifies that a
197 person made a vow or affirmation in the presence of the notary on penalty of perjury.

198 [15] (17) "Official misconduct" means a notary's performance of any act prohibited or
199 failure to perform any act mandated by this chapter or by any other law in connection
200 with a notarial act.

201 [16] (18)(a) "Official seal" means the seal described in Section 46-1-16 that a notary
202 may attach to a notarial certificate to complete a notarization.

203 (b) "Official seal" includes an electronic seal.

204 [17] (19) "Personally known" means familiarity with an individual resulting from
205 interactions with that individual over a period of time sufficient to eliminate every
206 reasonable doubt that the individual has the identity claimed.

207 [18] (20) "Remote notarization" means a notarial act performed by a remote notary in
208 accordance with this chapter for an individual who is not in the physical presence of the
209 remote notary at the time the remote notary performs the notarial act.

210 [19] (21) "Remote notary" means a notary that holds an active remote notary certification
211 under Section 46-1-3.5.

212 [20] (22)(a) "Satisfactory evidence of identity" means:

213 (i) for both an in-person and remote notarization, identification of an individual based
214 on:

215 (A) subject to Subsection [20](b) (22)(b), valid personal identification with the
216 individual's photograph, signature, and physical description that the United
217 States government, any state within the United States, or a foreign government
218 issues;

219 (B) subject to Subsection [20](b) (22)(b), a valid passport that any nation issues;
220 or

221 (C) the oath or affirmation of a credible person who is personally known to the
222 notary and who personally knows the individual; and

223 (ii) for a remote notarization only, a third party's affirmation of an individual's
224 identity in accordance with rules made under Section 46-1-3.7 by means of:

225 (A) dynamic knowledge-based authentication, which may include requiring the
226 individual to answer questions about the individual's personal information
227 obtained from public or proprietary data sources; or

228 (B) analysis of the individual's biometric data, which may include facial
229 recognition, voiceprint analysis, or fingerprint analysis.

230 (b) "Satisfactory evidence of identity," for a remote notarization, requires the
231 identification described in Subsection [20](a)(i)(A) (22)(a)(i)(A) or passport
232 described in Subsection [20](a)(i)(B) (22)(a)(i)(B) to be verified through public or
233 proprietary data sources in accordance with rules made under Section 46-1-3.7.

234 (c) "Satisfactory evidence of identity" does not include:

235 (i) a driving privilege card under Subsection 53-3-207(12); or

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

237 [(21)] (23) "Signature witnessing" means a notarial act in which an individual:

238 (a) appears in the presence of the notary and presents a document;

239 (b) provides the notary satisfactory evidence of the individual's identity, or is personally
240 known to the notary; and

241 (c) signs the document in the presence of the notary.

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

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

245 (b) maintains an immutable audit trail of authentication events.

246 Section 5. Section **57-3-101** is amended to read:

247 **57-3-101 . Certificate of acknowledgment, proof of execution, jurat, or other**
248 **certificate required -- Notarial acts affecting real property -- Right to record documents**
249 **unaffected by subdivision ordinances.**

250 (1) A certificate of the acknowledgment of any document, or of the proof of the execution
251 of any document, or a jurat as defined in Section 46-1-2, or other notarial certificate
252 containing the words "subscribed and sworn" or their substantial equivalent, that is
253 signed and certified by the officer taking the acknowledgment, proof, or jurat, as
254 provided in this title, or a digitally authenticated record as provided in Section
255 57-3-101.5, entitles the document and the certificate to be recorded in the office of the
256 recorder of the county where the real property is located.

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

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

262 Section 6. Section **57-3-101.5** is enacted to read:

263 **57-3-101.5 . Digital authentication as alternative to notarization.**

264 (1) As used in this section:

265 (a) "Digital authentication" means the same as that term is defined in Section 46-1-2.

266 (b) "Digitally authenticated record" means the same as that term is defined in Section
267 46-1-2.

268 (2) A digitally authenticated record has the same legal effect for recording purposes as a

269 document that contains a certificate of acknowledgment, proof of execution, jurat, or
270 other certificate described in Section 57-3-101 if:
271 (a) the digitally authenticated record meets the standards established by the State
272 Archivist under Section 63A-12-117; and
273 (b) if the digitally authenticated record is to be recorded by a county recorder, the county
274 has obtained approval under Section 17-71-301.5.

275 (3) This section does not:

276 (a) require a person to use digital authentication;
277 (b) invalidate a document authenticated by traditional notarization under Section
278 57-3-101; or
279 (c) require a county recorder to accept digitally authenticated records.

280 Section 7. Section **63A-12-101** is amended to read:

281 **63A-12-101 . Division of Archives and Records Service created -- Duties.**

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

283 (2) The state archives shall:

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

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

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

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

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

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

300 (g) provide staff and support services to the Records Management Committee created in
301 Section 63A-12-112 and the Government Records Office, created in Section
302 63A-12-202;

303 (h) develop training programs to assist records officers and other interested officers and
304 employees of governmental entities to administer this chapter and Title 63G, Chapter
305 2, Government Records Access and Management Act;
306 (i) provide access to public records deposited in the archives;
307 (j) administer and maintain the Utah Public Notice Website established under Section
308 63A-16-601;
309 (k) provide assistance to any governmental entity in administering this chapter and Title
310 63G, Chapter 2, Government Records Access and Management Act;
311 (l) prepare forms for use by all governmental entities for a person requesting access to a
312 record; [and]
313 (m) if the department operates the Division of Archives and Records Service as an
314 internal service fund agency in accordance with Section 63A-1-109.5, submit to the
315 Rate Committee established in Section 63A-1-114:
316 (i) the proposed rate schedule as required by Section 63A-1-114; and
317 (ii) other information or analysis requested by the Rate Committee[.] ; and
318 (n) establish standards for digital authentication systems and review county proposals
319 for accepting digitally authenticated records in accordance with Section 17-71-301.5.

320 (3) The state archives may:
321 (a) establish a report and directives management program;
322 (b) establish a forms management program; and
323 (c) in accordance with Section 63A-12-101, require that an individual undergo a
324 background check if the individual:
325 (i) applies to be, or currently is, an employee or volunteer of the division; and
326 (ii) will have direct access to a vulnerable record in the capacity described in
327 Subsection (3)(c)(i).

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

331 Section 8. Section **63A-12-104** is amended to read:

332 **63A-12-104 . Rulemaking authority.**

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

334 (1) the state archivist may make rules establishing:
335 (a) procedures for the collection, storage, designation, classification, access, mediation
336 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 9. 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 46-1-2.

(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;
- (iii) format sustainability for long-term preservation; and
- (iv) compliance with retention schedules.

Section 10. 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:

405 (i) to evaluate the adequacy of the division's and the executive branch agencies' data
406 and information technology system security standards; and
407 (ii) that will be completed over a period that does not exceed two years; and
408 (b) communicate the results of the assessment described in Subsection (4)(a) to the
409 appropriate executive branch agencies and to the president of the Senate and the
410 speaker of the House of Representatives;

411 (5) subject to Subsection 63G-6a-109.5(9):
412 (a) advise executive branch agencies on project and contract management principles as
413 they relate to information technology projects within the executive branch; and
414 (b) approve the acquisition of technology services and products by executive branch
415 agencies as required under Section 63G-6a-109.5;

416 (6) work toward building stronger partnering relationships with providers;
417 (7) develop service level agreements with executive branch departments and agencies to
418 ensure quality products and services are delivered on schedule and within budget;
419 (8) develop standards for application development including a standard methodology and
420 cost-benefit analysis that all agencies shall utilize for application development activities;
421 (9) determine and implement statewide efforts to standardize data elements;
422 (10) coordinate with executive branch agencies to provide basic website standards for
423 agencies that address common design standards and navigation standards, including:
424 (a) accessibility for individuals with disabilities in accordance with:
425 (i) the standards of 29 U.S.C. Sec. 794d; and
426 (ii) Section 63A-16-209;
427 (b) consistency with standardized government security standards;
428 (c) designing around user needs with data-driven analysis influencing management and
429 development decisions, using qualitative and quantitative data to determine user
430 goals, needs, and behaviors, and continual testing of the website, web-based form,
431 web-based application, or digital service to ensure that user needs are addressed;
432 (d) providing users of the website, web-based form, web-based application, or digital
433 service with the option for a more customized digital experience that allows users to
434 complete digital transactions in an efficient and accurate manner; and
435 (e) full functionality and usability on common mobile devices;
436 (11) consider, when making a purchase for an information system, cloud computing
437 options, including any security benefits, privacy, data retention risks, and cost savings
438 associated with cloud computing options;

439 (12) develop systems and methodologies to review, evaluate, and prioritize existing
440 information technology projects within the executive branch and report to the governor
441 and the Government Operations Interim Committee in accordance with Section
442 63A-16-201 on a semiannual basis regarding the status of information technology
443 projects;

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

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

450 (a) under this chapter;

451 (b) by the department; or

452 (c) by the division;

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

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

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

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

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

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

464 (a) control costs;

465 (b) ensure business value to a project;

466 (c) maximize resources;

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

468 (e) avoid duplication of resources;

469 (21) develop a method of accountability to agencies for services provided by the
470 department through service agreements with the agencies;

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

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

475 (24) provide services, including technical assistance:
476 (a) to executive branch agencies and subscribers to the services; and
477 (b) related to information technology or telecommunications;

478 (25) establish telecommunication system specifications and standards for use by:
479 (a) one or more executive branch agencies; or
480 (b) one or more entities that subscribe to the telecommunication systems in accordance
481 with Section 63A-16-302;

482 (26) coordinate state telecommunication planning, in cooperation with:
483 (a) state telecommunication users;
484 (b) executive branch agencies; and
485 (c) other subscribers to the state's telecommunication systems;

486 (27) cooperate with the federal government, other state entities, counties, and municipalities
487 in the development, implementation, and maintenance of:
488 (a)(i) governmental information technology; or
489 (ii) governmental telecommunication systems; and
490 (b)(i) as part of a cooperative organization; or
491 (ii) through means other than a cooperative organization;

492 (28) establish, operate, manage, and maintain:
493 (a) one or more state data centers; and
494 (b) one or more regional computer centers;

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

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

502 (31) establish standards for the information technology needs of a collection of executive
503 branch agencies or programs that share common characteristics relative to the types of
504 stakeholders the agencies or programs serve, including:
505 (a) project management;
506 (b) application development; and

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

508 (32) provide oversight of information technology standards that impact multiple executive

509 branch agency information technology services, assets, or functions to:

510 (a) control costs;

511 (b) ensure business value to a project;

512 (c) maximize resources;

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

514 (e) avoid duplication of resources;

515 (33) establish a system of accountability to user agencies through the use of service

516 agreements; [and]

517 (34) provide the services described in Section 63A-16-109 for a state elected official or

518 state employee who has been threatened[.]; and

519 (35) provide technical consultation to the State Archives regarding digital authentication

520 systems in accordance with Section 63A-16-215.

521 Section 11. Section **63A-16-215** is enacted to read:

522 **63A-16-215 . Digital authentication system technical support.**

523 (1) As used in this section:

524 (a) "Digital authentication system" means technology and procedures used to create

525 digitally authenticated records.

526 (b) "Digitally authenticated record" means the same as that term is defined in Section

527 46-1-2.

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

529 (d) "State Archives" means the Division of Archives and Records Service created in

530 Section 63A-12-101.

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

532 (a) security standards for digital authentication systems;

533 (b) cybersecurity requirements;

534 (c) authentication technologies and methods; and

535 (d) system integrity standards.

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

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

538 Section 12. **Effective Date.**

539 This bill takes effect on May 6, 2026.