

LEGISLATIVE COUNSEL AND JUDICIARY CHECKLIST

Matters Requiring Drafting or Committee Review

This checklist identifies drafting, reconciliation, implementation, and policy questions requiring Legislative Council or committee review as the South Carolina Digital Bill of Rights framework moves toward statutory implementation. Inclusion of an issue does not presume a particular legislative outcome; it identifies matters requiring deliberate resolution in final legislation.

Code Placement and Structure

- Determine final placement of the general digital-rights implementation chapter and necessary conforming amendments.
- Avoid duplicative definitions where existing Code definitions can be incorporated without weakening the framework.

Definitions

- Refine protected digital information, automated decision system, adverse governmental determination, high-consequence system, surveillance technology, material change, governmental entity, contractor, and third party.
- Keep high-consequence coverage tied to function, capability, operation, and effect rather than vendor labels.

Constitutional Floor

- State expressly that statutory compliance is not a safe harbor for unconstitutional conduct.
- Preserve independent protections of S.C. Const. art. I, §10.

Government by Proxy

- Use functional-equivalence language that prevents commercial availability, third-party possession, contracting, or shared-system access from independently creating governmental authority.

Law Enforcement and Emergencies

- Preserve constitutionally recognized warrant exceptions and carefully defined emergencies.

- Review §17-13-142 and Titles 17 Chapters 29 and 30 for state-constitutional savings clauses and modern definitions.

Data Minimization, Retention, and Disposition

- Determine appropriate purpose-limitation, minimization, retention, anonymization, and disposition requirements for protected digital information.
- Reconcile those requirements with public-record obligations, records-retention schedules, litigation holds, evidentiary duties, criminal investigations, court orders, program-specific requirements, and other independent legal preservation obligations.
- Avoid indefinite retention based solely on technological capability or storage convenience while preserving information that lawfully must be retained.

Individual Access, Accuracy, and Correction

- Determine when individuals should be permitted to inspect governmental information concerning themselves, challenge demonstrably inaccurate information, and obtain timely correction.
- Define appropriate exceptions for active investigations, security, confidentiality, protected third-party information, judicial records, and other circumstances in which access or correction would conflict with law or legitimate governmental functions.
- Address downstream correction when materially inaccurate information has been transmitted to or relied upon by another governmental system or recipient.

Biometric Information

- Determine whether enhanced safeguards for governmental collection, generation, use, retention, analysis, sharing, and disclosure of biometric information should be incorporated into the principal Act, companion legislation, or existing privacy law.
- Reconcile biometric protections with Title 30, Chapter 2, H.3404, law-enforcement authorities, identification functions, security needs, and other applicable law.
- Ensure definitions remain technology-neutral enough to address templates, embeddings, vectors, behavioral biometrics, and future biometric identification or persistent-recognition methods.

Automated Decisions

- Define when independent human review, notice, explanation, correction, and challenge are required.
- Protect legitimate investigative and security needs without allowing blanket automation exceptions.
- Specify the minimum characteristics of meaningful independent human review, including an identified human decision-maker with sufficient information and actual authority to

evaluate, reject, correct, or modify a material automated determination rather than merely ratify the system's output.

High-Consequence Systems

- Define independent verification and reconstructability by outcome/risk rather than mandating one technology.
- Determine appropriate exceptions where independent evidence is technologically impossible or disproportionate, with written findings and compensating safeguards.

Impact Assessments

- Determine which high-consequence governmental digital systems, surveillance technologies, automated decision systems, and material changes require an impact assessment before deployment, renewal, or continued use.
- Define minimum assessment content, including legal authority, constitutional and privacy implications, data sources, automated functions, human review, independent verification, cybersecurity, remote access, material foreign dependencies, cloud services, subcontractors, records, and anticipated effects on substantial legal interests.
- Determine appropriate treatment of confidential, security-sensitive, trade-secret, and law-enforcement information while preserving meaningful legislative, judicial, audit, inspector, and public accountability.

Procurement and Contractors

- Require audit/oversight access, records, material-change notice, cybersecurity duties, subcontractor transparency, remote-access disclosure, data disposition, and flow-down clauses.
- Clarify that procurement authority, contractual access, possession of technology, or technical capability does not independently create substantive governmental authority to use every capability of an acquired system.

Commercial Off-the-Shelf Components / Certification

- Determine appropriate disclosure, traceability, testing, update, remote-access, and material-change requirements for commercial off-the-shelf hardware, software, firmware, modules, libraries, and other components incorporated into high-consequence governmental systems.
- Ensure certification, accreditation, testing, procurement approval, or compliance with a technical standard does not, standing alone, create a conclusive presumption of correctness, integrity, security, lawful operation, or statutory compliance.

- Determine when independent verification must be capable of detecting a material error or compromise notwithstanding prior vendor, laboratory, governmental, or third-party certification or testing.

Foreign Dependencies

- Distinguish foreign manufacture from material foreign control or operational dependency.
- Define reportable remote administration, data access, update authority, authentication, cloud, and subcontractor dependencies.
- Determine appropriate risk-assessment, disclosure, mitigation, and oversight requirements where material foreign control, access, administration, update authority, authentication dependency, or other operational dependency could affect a high-consequence governmental function.

Public Records and Trade Secrets

- Preserve existing FOIA exemptions.
- Clarify that a public-disclosure exemption does not eliminate lawful court, legislative, audit, or inspector access.

Remedies and Immunities

- Resolve standing, injunctive/declaratory relief, preservation, attorney fees, civil remedies, suppression where appropriate, and interaction with governmental immunities.

Objective Standards

- Replace subjective operative terms with objective tests where practical, particularly for human review, emergency authority, material changes, auditability, and compliance triggers.

Audit Evidence

- Specify which covered systems must create audit evidence, required fields, retention periods, integrity controls, and vendor production obligations.

Independent Audits

- Determine whether designated categories of high-consequence governmental digital systems or surveillance technologies should be subject to periodic or event-triggered independent audits in addition to impact-assessment, independent-verification, and audit-evidence requirements.
- Define appropriate audit triggers, independence requirements, scope, access, records, frequency, reporting, remediation, and treatment of confidential or security-sensitive information.

Public Technology Inventory

- Determine whether public technology inventories should remain maintained by individual governmental entities as provided in the proposed Act or whether the State should additionally provide a centralized public reporting or searchable mechanism.
- Determine minimum inventory fields, update frequency, treatment of materially changed systems, and narrow exclusions necessary to protect legitimate investigative or security interests without defeating meaningful transparency.

State-Agency Surveillance Authorization

- Determine whether an affirmative-authorization mechanism analogous to the political-subdivision process should apply when a State agency proposes to deploy a new category of surveillance technology or a materially new use of existing surveillance technology and, if so, what authorization, notice, review, and accountability process is appropriate to State-agency governance.

Statewide Oversight

- Determine whether existing oversight authorities are sufficient to administer and oversee statewide compliance or whether additional jurisdiction, designation of a lead oversight entity, or another coordination mechanism is warranted.
- Consider the appropriate roles, if any, of existing inspectors, auditors, procurement authorities, legislative oversight bodies, courts, or another designated entity without unnecessarily duplicating existing jurisdiction.

Renewals / Material Changes / Legacy Systems

- Define transition periods and event triggers so legacy status does not become indefinite grandfathering; distinguish routine maintenance from material capability changes.

Anti-Circumvention

- Confirm that paid and unpaid access, third-party queries, shared/federated systems, derived information, and divided governmental functions cannot be used to evade otherwise applicable duties.

Local Government / Home Rule

- Determine which duties apply statewide to political subdivisions and how local authorization requirements interact with home-rule authority.

Children's Digital Rights

- Reconcile the Digital Bill of Rights framework with H.3400 and other applicable state and federal protections governing children's data, education records, parental authority, child protection, and online services.
- Determine which protections should apply specifically to governmental collection, generation, use, retention, sharing, profiling, biometric processing, persistent identification, or automated decision-making involving minors.
- Preserve legitimate educational, health, safety, child-protection, and other lawful governmental functions while establishing appropriate safeguards for children's protected digital information.

Image, Voice, Likeness, and Photo Consent

- Reconcile H. 3404 with the Digital Bill of Rights without converting the presence of a person in a photograph or recording into ownership of the expressive work.
- Define the relationship among consent, commercial exploitation, synthetic or biometric use, minors, news and public-interest uses, ordinary photography and recording, and constitutional speech and press protections.
- Clarify that protected digital information may be contained in or derived from an expressive work without transferring ownership of the work.

Open Fields / Private-Land Surveillance

- Review S.C. Code §50-3-420 and the scope of governmental investigative entry onto posted and unposted private property beyond curtilage.
- Determine the statutory rule for physical entry, installed or placed surveillance equipment, unmanned aircraft, remote sensing, owner consent, warrants, emergencies, and other lawful authority.
- Coordinate remedies with Section [--160] of the proposed Digital Liberty and Government Technology Accountability Act while distinguishing suppression or exclusion issues from civil and equitable remedies.

Transition and Fiscal Impact

- Establish prospective application, treatment of renewals/material changes, legacy-system transition periods, and reasonable implementation deadlines.
- Identify fiscal effects of inventories, audit logs, procurement clauses, incident response, and oversight.
- Consider phased or proportionate compliance mechanisms for smaller political subdivisions where appropriate without creating permanent exemptions from core constitutional or accountability requirements.

Federal Law

- Identify areas governed by federal communications, disability-access, criminal-procedure, grant, or procurement requirements and include savings clauses accordingly.
- Review applicable federal electronic-communications, stored-communications, interception, pen-register/trap-and-trace, motor-vehicle-record, education, children's privacy, and other federal requirements implicated by final implementation language.
- Identify preemption, federal-funding, interoperability, or other federal-law constraints without treating federal minimum requirements as a ceiling on protections South Carolina may lawfully provide.