LEGISLATIVE WORKING DRAFT

Idaho Mass Surveillance Voter Authorization Act

VERSION 3.2

Walter Boyd · October 20, 2026

Proposed legislation for legal and fiscal review.

Not introduced in the Idaho Legislature.

Contents

01 Purpose and Legislative Findings

02 Definitions

03 Mandatory Voter Authorization

04 Election Scheduling and Reauthorization

05 Territorial Authorization

06 Existing Systems

07 Exempt Recording Systems

08 Government Facility Security Limitations

09 Permitted Surveillance Searches and Investigative Authorization

10 Protected Activities and Improper Targeting

11 Retention and Deletion

12 Vendor Responsibilities and Technical Controls

13 Data Sharing, Acquisition, and Anti-Circumvention

14 Public Disclosure and Ballot Requirements

15 Independent Auditing, Misuse Detection, and Notification

16 Enforcement, Civil Penalties, and Individual Remedies

17 Judicial Prohibitions and Reinstatement

18 Public Records and Confidentiality

19 Conforming Amendments

20 Construction and Severability

Section 1. Purpose and Legislative Findings

The purpose of this act is to protect the privacy and constitutional liberties of Idaho residents by requiring informed, affirmative, and periodically renewed voter authorization before government agencies conduct systematic mass surveillance of the public.

The Legislature recognizes that technologies capable of continuously identifying individuals, vehicles, locations, and associations create privacy risks substantially different from ordinary security recording and evidence collection during individual investigations.

The Legislature further recognizes that automated surveillance systems are vulnerable to unauthorized access, personal misuse, inaccurate identification, improper data sharing, and circumvention of institutional controls.

Voter authorization shall constitute an additional statutory protection and shall not replace rights guaranteed by the United States Constitution, the Idaho Constitution, or other applicable law.

The Legislature further finds that systematic government surveillance of the general public presents a fundamental question of democratic consent, distinct from the operational judgment of a law enforcement or government agency. The decision whether to authorize such surveillance belongs to the qualified electors of the affected community.

(a) Government ownership, technological capability, investigative utility, and appropriated funds do not independently establish public authorization to conduct covered mass surveillance.

(b) The election of public officials does not substitute for the system-specific approval required by this act.

(c) Public authorization must be affirmative, informed, geographically applicable, limited in scope, and periodically renewed.

(d) Except for the expressly limited transition for existing lawful systems in Section 6, the absence of affirmative authorization constitutes the absence of legal authority to operate, not permission to continue operating pending a future vote.

(e) Voter approval permits only the activities disclosed and approved; it does not waive constitutional rights, warrants, judicial oversight, or other statutory protections.

(f) Public consent is continuing rather than perpetual; authorization expires unless renewed as prescribed by this act.

The governing principle of this act is that covered government mass surveillance is prohibited unless the affected electorate affirmatively authorizes it, subject only to the express transition in Section 6.

Section 2. Definitions

(1) Covered mass-surveillance system. Any device, software, database, network, or service operated by, for, or made routinely accessible to a government agency that systematically identifies, matches, indexes, monitors, or tracks persons or vehicles without individualized suspicion.

Covered systems include automated license-plate readers, automated facial-recognition systems, device-identifier tracking, and substantially equivalent technologies.

(2) Single-device applicability. One device performing a covered surveillance function constitutes a covered system. Coverage shall not depend on device quantity, installation location, mobility, connectivity, data-sharing arrangements, storage location, or retention duration.

(3) Surveillance data. Images, recordings, identifiers, timestamps, locations, automated matches, historical movements, inferred associations, derived

profiles, and other identifying information collected or generated through a covered system.

(4) Government agency. Any Idaho state or local governmental entity, law enforcement organization, political subdivision, joint governmental operation, or contractor acting on its behalf.

(5) Affected jurisdiction. The incorporated municipality or unincorporated county territory deliberately subjected to covered surveillance.

(6) Qualifying election. The regularly scheduled statewide general election held in November of an even-numbered year.

(7) Presidential election. The November general election held in a year in which presidential electors are selected.

(8) Valid authorization. Affirmative approval by a majority of votes cast on the applicable ballot question, within its approved scope and effective term.

(9) Material expansion. Any significant increase in surveillance territory, approved device quantity, identification capabilities, authorized uses, participating agencies, or database connectivity beyond the scope previously approved by voters.

(10) Retrospective search. A query intended to identify, reconstruct, analyze, or establish a person's or vehicle's previous locations, movements, contacts, or associations.

(11) Biometric identification. Automated analysis, comparison, or matching of a person’s facial characteristics, iris, voice, gait, or other biological or behavioral characteristics for the purpose of identifying or verifying a person, including use of biometric templates or identifiers derived from recordings.

(12) Association mapping. Automated identification, indexing, correlation, or analysis of persons' co-presence, repeated encounters, shared attendance, contacts, affiliations, or inferred social, political, religious, or other relationships through surveillance data, alone or combined with other databases.

(13) Real-time biometric identification. Contemporaneous comparison of biometric characteristics in a live or near-live camera or sensor feed against stored images, identifiers, templates, or watchlists for the purpose of identifying a person.

(14) Generalized biometric identification. Identification or attempted identification of persons indiscriminately, or compilation of an identity or attendance register, rather than a particularized comparison undertaken for an independently documented, lawful purpose. This term includes systematic identification of attendees of a gathering or persons passing through a public location without an individualized investigative basis.

Section 3. Mandatory Voter Authorization

(1) No government agency shall activate or operate a covered mass-surveillance system without valid voter authorization, except as expressly provided for existing systems during the transition period.

(2) Authorization shall be required for a single covered device, whether networked or independent.

(3) Authorization shall be specific to the system, functions, agencies, and territory disclosed to voters.

(4) No general assertion of crime prevention, public safety, missing-person recovery, human trafficking prevention, investigative necessity, or operational preference shall waive this requirement.

(5) Emergency circumstances shall not permit activation, reactivation, or continued operation of a system lacking valid voter authorization.

(6) Lawful emergency alerts, targeted investigations, and case-specific evidence gathering remain permissible independently of unauthorized mass-surveillance systems.

(7) Voter authorization is a condition precedent. Except for the express transition in Section 6, affirmative voter approval is an indispensable prerequisite to operation. Judicial warrants, technical safeguards, agency policies, audits, or vendor agreements shall not substitute for that approval.

(8) No administrative substitute. No county commission, city council, sheriff, police chief, governor, state agency, contractor, or other public official may grant, extend, or substitute for voter authorization required by this act.

(9) No implied consent. Public silence, previous operation, prior expenditure of public funds, vendor contracts, agency practice, absence of public objection, or election of an official shall not constitute authorization.

(10) Scope of consent. Approval covers only the disclosed technology, purposes, capabilities, participating agencies, maximum device deployment, and authorized territory. It does not itself require an agency to purchase, fund, activate, or continue the system.

(11) Preservation of superior legal limits. An affirmative vote does not authorize surveillance otherwise prohibited by the United States Constitution, the Idaho Constitution, controlling judicial orders, or applicable law.

Section 4. Election Scheduling and Reauthorization

(1) Initial authorization shall be sought at the next qualifying November general election for which applicable ballot-submission deadlines can be satisfied.

(2) No May election, odd-year November election, or special election shall be conducted for purposes of this act.

(3) Every authorization shall require renewal at the next presidential general election and every subsequent presidential general election.

(4) Authorization granted at an intervening midterm general election shall remain valid only until the next presidential general election unless lawfully terminated earlier.

(5) Rejection, failure to obtain a majority affirmative vote, or failure to submit a required renewal question shall terminate authorization upon certification of the applicable election.

(6) An agency may seek authorization at a subsequent qualifying election but shall not operate its system without valid authorization in the interim.

(7) Elections shall use existing general-election infrastructure and procedures, subject to the specific administrative provisions established by this act.

(8) No governing body, public official, or agency may reverse, suspend, disregard, or administratively extend a rejection, expiration, or nonrenewal of voter authorization by ordinance, resolution, contract, intergovernmental agreement, or other action that is not itself valid voter authorization under this act.

(9) Following expiration or certified rejection, the responsible agency shall direct its contractors and vendors to disable continuing unauthorized collection, access, processing, and searching consistent with the shutdown, preservation, and evidentiary requirements elsewhere in this act.

(10) Authorization constitutes temporary permission within the approved scope, not permanent entitlement. No asserted operational emergency shall permit an off-cycle election or continuation of an unauthorized covered system contrary to this act.

Section 5. Territorial Authorization

(1) Surveillance deliberately conducted within an incorporated municipality shall require authorization from that municipality's qualified electors.

(2) Surveillance deliberately conducted within unincorporated county territory shall require authorization from qualified electors residing in the affected unincorporated territory, under election procedures established for that purpose.

(3) State agencies, county sheriffs, municipal police departments, contractors, and joint governmental operations shall be subject to authorization requirements applicable to the territory surveilled.

(4) Approval in one jurisdiction shall not override rejection or absence of approval in another.

(5) Deliberate surveillance of territory outside the jurisdiction where equipment is installed shall require authorization applicable to the territory surveilled.

(6) Participating agencies and their access rights shall be identified in the authorization proposal. New participating agencies or materially broader network access shall require voter approval.

(7) Nothing in this act purports to regulate independent federal or tribal sovereign operations beyond Idaho's lawful authority.

Section 6. Existing Systems

(1) Systems lawfully operating on the effective date may continue operating until certification of the first qualifying election for which applicable ballot deadlines can be met.

(2) Existing systems may not materially expand during this transition without voter authorization.

(3) Failure to obtain approval at the required election shall terminate transitional operating authority.

(4) Judicial orders prohibiting operation shall take precedence over transitional authorization.

(5) Termination of a judicial prohibition shall not automatically revive expired transitional authority.

(6) Initial voter ratification. At the first qualifying election required under subsection (1), the affected electorate shall decide whether an existing covered system may continue operating, regardless of prior approval by a sheriff, police chief, governing body, or other official.

(7) An affirmative majority vote at that election authorizes continued operation only within the approved and disclosed scope, and subject to every other requirement of this act. That vote shall not retroactively excuse any unlawful surveillance, access, retention, or disclosure before the election.

(8) A failure to obtain an affirmative majority vote terminates the authority of the existing system to operate upon certification of the election results. No official, agency, or contractor may extend, override, or disregard that decision.

(9) A rejected existing system may not resume operation until subsequently authorized at a qualifying election. The transition permission in subsection (1) is a one-time exception and does not revive following rejection, expiration, or a court-ordered shutdown addressed by subsection (5).

Section 7. Exempt Recording Systems

The voter-authorization requirements shall not apply to:

(a) Police body-worn cameras documenting official duties and encounters.

(b) Police vehicle cameras documenting traffic stops, pursuits, arrests, accidents, prisoner transport, and other official activities.

(c) Private security and operational cameras used by private persons, businesses, and agricultural enterprises for lawful property protection, security, safety, livestock monitoring, agricultural management, or operational purposes.

This includes homes, commercial premises, farms, orchards, ranches, dairies, livestock facilities, poultry operations, grazing allotments, and agricultural activities conducted on lawfully used public land.

(d) Government facility security cameras permanently installed to protect legitimate government buildings, their occupants, equipment, entrances, grounds, and associated premises.

(e) Event-triggered traffic enforcement cameras that capture particular apparent violations without retaining or indexing identifying records of motorists who have committed no violation.

(f) Nonidentifying monitoring systems collecting aggregate traffic, infrastructure, environmental, or operational information.

(g) Case-specific evidence voluntarily provided or lawfully obtained from otherwise exempt recording systems.

Incidental recording of public places shall not, by itself, invalidate an exemption.

No exemption shall authorize an otherwise exempt camera system to be repurposed into a government-operated system for systematic identification or

tracking of the general public.

Section 8. Government Facility Security Limitations

(1) A government building must be a bona fide structure primarily intended for human occupancy or government operations.

(2) Camera poles, utility poles, equipment cabinets, and structures principally intended to support surveillance equipment shall not qualify as government buildings.

(3) Government ownership, administrative designation, or reclassification shall not establish eligibility for the exemption.

(4) Cameras mounted on legitimate government buildings shall remain subject to voter authorization if used for covered mass-surveillance functions.

(5) Mobile equipment, including unmanned aircraft, shall not qualify solely under the fixed-facility exemption.

Section 9. Permitted Surveillance Searches and Investigative Authorization

(1) Judicial warrants. A retrospective search intended to identify or reconstruct a person's or vehicle's historical locations, movements, or associations shall require a judicial warrant supported by probable cause.

(2) Particularity. Warrants shall identify the investigative purpose, relevant person or vehicle identifiers, geographic area, and authorized time period with reasonable particularity.

(3) Contemporaneous alerts. A lawfully authorized system may perform narrowly defined real-time comparisons against specifically approved

investigative or missing-person alerts, consistent with existing law and voter-approved purposes.

(4) Individual authentication. Every user shall access the system through individually assigned credentials using multifactor authentication where technically feasible. Shared accounts are prohibited.

(5) Verified investigative authorization. Every retrospective query shall be associated with a verifiable warrant or judicial authorization and an independently maintained investigation identifier. Entry of free-form text, an invented case number, or an unverified purpose code shall not constitute sufficient authorization.

(6) Independent authorization records. The surveillance system shall validate required investigative authorization against records maintained outside the surveillance vendor's ordinary query interface.

(7) Emergency searches. When an imminent threat to human life makes prior judicial authorization impracticable, a limited search of lawfully collected data may proceed upon documented emergency justification.

Emergency searches shall be subject to supervisory review, prompt subsequent judicial review, and independent audit.

(8) No emergency deployment exception. An emergency may justify a lawful search of an authorized system, but shall never authorize operation of a system lacking valid voter approval.

(9) Automated matches. An automated match shall be treated as an investigative lead, not conclusive identification or independent authority for detention or arrest.

(10) Independent verification. Before enforcement action substantially relying on an automated match, an officer shall take reasonable steps to verify identifying information, including relevant license-plate characters, issuing

jurisdiction, vehicle characteristics, current alert status, and available corroborating evidence.

Any exigent-circumstances exception shall require independently documented circumstances and shall not arise solely from the automated match.

(11) Targeted real-time biometric alerts. A contemporaneous biometric identification alert shall be limited to a specifically identified person associated with a documented, lawful, and particularized investigation or a valid missing-person or endangered-person alert. The responsible agency shall independently record the target identity, lawful basis, permissible use, approving official, scope, and expiration or review date of the alert. An unrestricted watchlist, generalized public-safety objective, or unverified external designation alone shall not establish sufficient authorization. Judicial authorization shall be obtained whenever required by the Constitution or applicable law.

(12) Prohibition on generalized identification. A covered system shall not be used for generalized real-time biometric identification, compilation of identity or attendance rosters, or continuous identification of persons in public places or at lawful gatherings without individualized investigative justification. A targeted comparison satisfying subsection (11) remains subject to Section 10 and all voter-authorization requirements.

(13) Biometric-match verification. A biometric match shall be treated only as an investigative lead. Before an enforcement action substantially relying on the match, an officer shall perform and document reasonable independent verification of identity, relevant image or signal quality, the currency and accuracy of the source record, known potential for erroneous matches, and available corroborating evidence. A match alone shall not supply authority for detention, arrest, or another adverse action. Any exigent action shall require independently documented circumstances and shall not rest solely on the match.

(14) Protected-location limitation. Biometric matching shall not be used to identify or catalogue persons because they attend a demonstration, political meeting, religious service, healthcare facility, or other protected gathering. A targeted investigation based on independently established facts concerning specific unlawful conduct may proceed only within the scope authorized under this section and Section 10.

Section 10. Protected Activities and Improper Targeting

(1) No surveillance system shall be used to identify, monitor, or investigate persons solely because of their participation in lawful political activity, public demonstrations, religious observance, lawful healthcare, protected association, or exercise of constitutional rights.

(2) No person shall be selected for surveillance solely because of race, ethnicity, religion, national origin, or another characteristic protected by applicable law.

(3) Surveillance access shall require lawful investigative justification independent of protected activity or personal characteristics.

(4) This section shall not prevent investigations supported by independently established facts concerning specific unlawful conduct.

(5) Searches intended to identify demonstrators, attendees at political meetings, visitors to sensitive facilities, or members of particular associations without proper investigative authorization are prohibited.

(6) Prohibition on association registers. A government agency or its contractor shall not use a covered system to compile, maintain, retrieve, or analyze lists of participants, attendance profiles, relationship graphs, organizational affiliations, or inferred associations arising from lawful political, religious, healthcare, labor, charitable, or similarly protected activities without

particularized investigative justification independent of the protected activity and any judicial authorization required by Section 9.

(7) Investigative minimization. A lawful, case-specific investigation shall not justify bulk identification of other attendees or associates who lack an independent investigative connection. Searches and analytical outputs shall be confined to the persons, conduct, places, and periods reasonably relevant to the authorized investigation, and unnecessary disclosure of uninvolved persons' identities or associations is prohibited.

(8) Indirect inference prohibited. Restrictions in this section apply equally when affiliation, participation, attendance, or relationships are inferred through repeat co-location, vehicle records, biometric information, device identifiers, linked databases, contractors, or third-party analytics rather than directly recorded.

Section 11. Retention and Deletion

(1) Identifying surveillance data unrelated to specific lawful investigations shall be deleted within twenty-one days of collection.

(2) The limitation applies to images, plate records, metadata, searchable indexes, replicated records, inferred associations, derived profiles, and vendor-controlled copies.

(3) Particular records may be preserved beyond twenty-one days only when required by lawful investigative preservation authority, judicial process, litigation holds, or other controlling evidence obligations.

(4) Preservation shall be limited to relevant records and shall not authorize retention of unrelated observations.

(5) Upon expiration of the applicable preservation obligation, retained records shall be deleted under the governing retention schedule.

(6) Termination of voter authorization requires cessation of new collection and ordinary searching. Preserved evidentiary records shall be segregated from operational surveillance systems.

(7) Technical audit logs may be retained for two years for accountability, subject to restrictions preventing their use as a substitute location-history database.

(8) Vendors shall certify deletion from operational databases, replicas, and backups under independently verifiable procedures.

(9) Conforming exceptions shall be established to Idaho's existing governmental records-retention requirements for routine, non-evidentiary surveillance data.

(10) Biometric and associational derivatives. Biometric templates, automated identity indexes, attendance profiles, relationship graphs, and inferred associations derived from covered surveillance data are subject to the same deletion deadline as their underlying routine identifying observations, calculated from the original collection date. Derivation, copying, export, or recomputation shall not restart the retention period. Preservation under subsection (3) remains available for specifically relevant evidence.

(11) No substitute archive. An agency or vendor shall not preserve otherwise-deletable identifying or associational surveillance information by converting it into biometric templates, relationship scores, hashes that permit reidentification, derived profiles, or another searchable representation.

Section 12. Vendor Responsibilities and Technical Controls

Every contract for a covered system shall require:

(1) Individually authenticated access and enforceable role-based permissions.

(2) Default-deny external sharing.

(3) Tamper-evident records of searches, exports, alerts, permission changes, and administrative activity.

(4) Validation of retrospective investigative authorization through independently maintained records.

(5) Detection of unusual search patterns, including repeated searches involving the same person or vehicle, unusually broad geographic queries, excessive access frequency, unusual after-hours access, and inconsistent investigative justifications.

(6) Independent examination of flagged activity, without giving the person whose conduct is questioned exclusive authority to resolve the alert.

(7) Prohibition on vendor demonstrations, sales presentations, employee training, or product testing using identifiable records of real persons without specific lawful authorization.

Synthetic or appropriately anonymized information shall be used for routine demonstrations and testing. Controlled security testing involving real records must follow separately documented, narrowly limited, independently auditable procedures.

(8) Prohibition on unauthorized resale, secondary use, retention, or disclosure of surveillance information.

(9) No changes to sharing permissions, external access rights, or substantive surveillance capabilities without documented agency approval consistent with voter authorization.

(10) Agency and independent-auditor access to complete compliance records.

(11) Prompt shutdown and access revocation when operating authority expires or is prohibited by court order.

(12) Independent verification of material shutdowns and required data deletion.

(13) Contractual termination rights implementing voter decisions, without penalties solely for complying with this act in contracts executed or renewed after its effective date.

(14) Preservation of records relevant to suspected vendor misconduct.

(15) Appropriate contractual remedies, indemnification provisions, and vendor-funded compliance examinations following material violations.

(16) Biometric operational safeguards, where such functions are approved, including documented alert approval and expiration, recording of match quality and human verification, periodic testing for erroneous identifications, and independent examination of material limitations.

(17) Technical and organizational controls preventing creation or use of generalized biometric-identification registers or prohibited association maps, with independently auditable records of configuration, searches, analytical outputs, exports, and changes to biometric and correlation capabilities.

(18) Disclosure to the responsible agency and independent auditor of system functions capable of identifying participants in gatherings, correlating encounters, inferring associations, or linking biometric identities with plate, device, location, or other databases, whether performed locally, remotely, or by a vendor.

Existing contracts shall not authorize operation prohibited by statute. Any liability arising from contracts executed before the act takes effect shall be evaluated under applicable contract law.

Section 13. Data Sharing, Acquisition, and Anti-Circumvention

(1) Government agencies shall not provide outside entities with standing, unrestricted, reciprocal, or bulk access to covered surveillance data.

(2) No agency may purchase, rent, license, or otherwise obtain automated access to privately assembled movement-history databases to evade voter authorization or judicial safeguards.

(3) Disclosure of specified surveillance records to outside entities shall require lawful, case-specific compulsory process, including a probable-cause warrant where required by this act.

(4) Narrow emergency disclosure of lawfully collected evidence may occur when necessary to address an imminent threat to human life, subject to documentation and subsequent review.

(5) Proxy searches conducted for entities lacking independent authority to obtain the same information are prohibited.

(6) Agencies shall not evade this act through contractors, other jurisdictions, joint task forces, private vendors, reciprocal arrangements, or transferred system ownership.

(7) Privately owned security cameras shall remain exempt unless their data is made routinely available to government for covered systematic identification or tracking.

(8) Case-specific voluntary disclosure or lawful acquisition of particular private recordings shall remain permissible.

(9) No contractual provision or local voter authorization shall waive the restrictions on unauthorized outside access.

(10) Nothing in this act shall prohibit compliance with controlling federal law or valid compulsory judicial process.

Section 14. Public Disclosure and Ballot Requirements

Before initial authorization and each renewal, the responsible agency shall publish:

(1) System purposes, capabilities, and technologies;

(2) Participating agencies, vendors, and contractors;

(3) Proposed territory and maximum device count;

(4) Collection categories and permitted uses;

(5) Retention, sharing, and access policies;

(6) Initial, recurring, and projected termination costs;

(7) Aggregate records of searches, alerts, verified investigative results, false matches, access violations, and remedial actions;

(8) Material changes since the preceding authorization;

(9) Findings from independent compliance examinations; and

(10) A summary of any substantial surveillance-related litigation or enforcement action.

(11) Whether real-time or retrospective biometric identification is available or proposed, the categories of biometric identifiers used, target-list sources, circumstances in which matches may be generated, match-verification procedures, known technical limits, and available documented error measurements;

(12) Whether the system can generate attendance lists, repeated-encounter records, co-location analyses, relationship graphs, inferred organizational affiliations, or other associational profiles, including through cross-database correlation or vendor services; and

(13) Specific controls, access restrictions, auditing, and investigative-authorization requirements intended to prevent generalized biometric identification and improper tracking of constitutionally protected activities.

Ballot wording shall identify the proposed surveillance system and explain the temporary nature of authorization.

Material expansion shall require additional voter approval.

Routine maintenance and functionally equivalent equipment replacement within the approved scope shall not require a separate vote.

The authorization ballot question shall identify the described system, participating agencies, intended uses, territory, and temporary authorization period. It shall plainly explain that an affirmative vote permits the disclosed system to operate subject to legal restrictions and that a negative vote denies the requested authority.

The public disclosures required by this section shall also describe anticipated public-safety benefits, known privacy and civil-liberties risks, and the applicable statutory restrictions, audit obligations, and legal remedies. They shall distinguish documented results from projected benefits and disclose material limitations, including verified false identifications or misuse when available. Official explanatory materials must present these matters factually rather than imply that a claimed benefit overrides the requirement for consent.

Separate surveillance systems capable of independent operation shall not be combined into a single ballot question solely to force voters to accept one

system as the condition for approving another.

The absence of a ballot question, an unapproved material expansion, or inadequate approval under this act shall not be treated as implied voter consent.

Section 15. Independent Auditing, Misuse Detection, and Notification

(1) Audit records. All users, including sheriffs, police chiefs, dispatchers, civilian analysts, system administrators, and vendor employees, shall be subject to equivalent audit requirements.

(2) Mandatory logging. Logs shall preserve user identity, role, agency, date, time, purpose, verified investigative authorization, search parameters, results accessed, exports, and permission changes.

(3) Semiannual audits. Surveillance systems shall undergo semiannual examination of access activity, with targeted review of suspicious transactions and a risk-based sample of apparently routine transactions.

(4) Independent examination. Audit findings involving potential personal misuse, supervisory misconduct, vendor wrongdoing, or systematic unauthorized access shall be reviewed by personnel independent of the implicated chain of command and vendor operations.

(5) Automated detection. Systems shall flag recurring searches of particular persons or vehicles, unexplained query volume, suspicious access patterns, false case references, abnormal vendor activity, and potential policy circumvention.

(6) Mandatory referral. Credible evidence of intentional misuse shall be preserved and referred to an independent enforcement authority or

appropriate court process. A sheriff or other implicated supervisor shall not possess unilateral authority to dismiss the matter.

(7) Vendor examinations. Following a material systemic violation, a court may require an independent technical and compliance examination at the responsible vendor's expense.

(8) Annual certification. Each agency shall publish an annual compliance certification identifying significant findings, remedial measures, and outstanding deficiencies.

(9) Pre-election report. Before presidential-year reauthorization, the agency shall disclose material audit findings accumulated during the preceding authorization term.

(10) Victim notification. When unauthorized access or disclosure affecting an identifiable person is substantiated, the responsible agency shall notify that person within thirty days of substantiation, unless delayed by court order.

(11) Delayed notification. A court may authorize a limited delay upon particularized findings that immediate notice would create a substantial risk to safety or a legitimate ongoing investigation. Extensions shall require renewed judicial justification.

(12) Notice content. Notification shall describe the general nature and approximate dates of unauthorized access, categories of information involved, responsible agency, and available legal remedies, without unnecessarily disclosing protected investigative information.

(13) Preservation. Allegations of unauthorized access shall trigger preservation of relevant authentication records, queries, exports, administrative changes, and associated investigation records.

(14) Biometric and association safeguards. Independent audits shall examine configurations, target-list authorizations, match-verification records,

erroneous-match findings, exports, identity or attendance listings, association analyses, and cross-database queries where such capabilities are present. Auditors shall assess whether technical use conforms to voter disclosures and Sections 9 and 10.

(15) Substantiated violations involving improper biometric identification or protected association mapping shall be included in the annual compliance certification and subject to the referral, preservation, and notification requirements of this section, with identifying details protected as required by law.

Section 16. Enforcement, Civil Penalties, and Individual Remedies

(1) Unauthorized operation. Operating a covered system without valid voter authorization constitutes a statutory violation.

(2) Injunctive relief. Courts may order immediate cessation of unlawful collection, searching, sharing, or retention and may require verified compliance.

(3) Vendor negligence. A commercial vendor or contractor committing a material negligent violation may be assessed a civil penalty of up to $100,000 per distinct violation.

(4) Knowing or reckless vendor misconduct. Deliberate unauthorized sharing, falsified audit records, unlawful data brokerage, intentional circumvention, or continued operation after mandatory shutdown may result in civil penalties of up to $1,000,000 per distinct violation.

(5) Systemic vendor misconduct. For repeated or systemic knowing violations, a court may impose an enhanced aggregate civil penalty of up to ten percent of the vendor's preceding annual United States revenue attributable to

covered surveillance products and services, in lieu of overlapping per-violation aggregate penalties as provided by statute.

The court shall consider culpability, duration, consequences, actual access or disclosure, prior violations, remedial action, and proportionality.

(6) Continuing noncompliance. After formal notice and an opportunity to comply, knowing continued violation may incur additional civil penalties of up to $25,000 per day, subject to judicial assessment.

(7) Individual civil penalties. Any sheriff, police chief, law enforcement officer, dispatcher, civilian employee, analyst, contractor, vendor employee, or other authorized user who willfully violates this act may be personally assessed up to $50,000 per distinct willful violation.

(8) Prohibited individual misconduct. Willful violations include:

(a) Accessing surveillance data for personal purposes;

(b) Monitoring a spouse, former spouse, intimate partner, former partner, family member, acquaintance, or other person without legitimate investigative authorization;

(c) Accessing records for political, retaliatory, discriminatory, or other prohibited purposes;

(d) Fabricating case numbers, warrants, investigative explanations, or audit records;

(e) Sharing credentials or accessing records under another person's identity;

(f) Disclosing information to unauthorized third parties;

(g) Performing prohibited proxy searches;

(h) Circumventing voter authorization or a judicial shutdown;

(i) Knowingly disabling access controls or misuse detection; or

(j) Directing, concealing, materially facilitating, or deliberately approving prohibited conduct.

(9) Rank-independent liability. Liability shall depend on the person's own culpable conduct, regardless of rank or employment classification. Supervisory status alone shall not establish personal liability.

(10) Personal financial responsibility. Individual statutory civil penalties shall be the personal obligations of the responsible persons and shall not be paid or reimbursed with public funds, to the extent permitted by controlling law.

(11) Vendor disqualification. Following repeated or systemic intentional misconduct, a court may prohibit the responsible vendor from entering into new Idaho government surveillance contracts for up to five years. Reinstatement may require independently verified remediation.

(12) Victim civil remedies. A person subjected to knowing unauthorized surveillance access may seek actual compensatory damages or statutory damages of $1,000 per distinct willful course of misconduct, whichever is greater, together with appropriate equitable relief and reasonable attorney fees.

Statutory damages shall not automatically multiply with each duplicate search, camera observation, or database replication absent a distinct actionable violation.

(13) Public enforcement. The Idaho Attorney General, county prosecuting attorneys, and duly authorized municipal attorneys shall have concurrent civil enforcement authority within their lawful jurisdictions.

(14) Independent private enforcement. A person subjected to unlawful surveillance, or a qualified elector whose jurisdiction's voter-authorization requirement has been violated, may seek declaratory and injunctive relief

without prior approval from a public enforcement official, subject to applicable standing requirements.

(15) Attorney fees. Prevailing private claimants may recover reasonable attorney fees and costs as provided by this act. Defendants may recover fees for demonstrably frivolous or bad-faith proceedings.

(16) Citizen-relator enforcement. The Legislature intends to establish a procedure, subject to constitutional review, permitting qualified private claimants to pursue judicial assessment of public civil penalties where responsible public authorities decline enforcement.

Any such procedure shall require express statutory standing, notice, judicial supervision, safeguards against duplicate recovery, and protection of defendants' due-process rights.

No enforcement official shall possess an unrestricted veto over independently authorized private compliance actions.

(17) Conflicts of interest. A public official implicated in alleged misconduct shall not control an independent investigation or legal proceeding addressing that conduct.

(18) Whistleblower protection. Retaliation against employees or contractors reporting suspected surveillance violations in good faith, preserving relevant evidence, or assisting lawful investigations is prohibited.

(19) Independent audits and remediation. Courts may require vendor-funded technical review and independently verified corrective action following serious violations.

(20) Nonexclusive remedies. Civil penalties do not preclude otherwise applicable criminal prosecution, employment discipline, contractual remedies, or constitutional claims.

(21) Constitutional proportionality. Penalties shall be imposed only after appropriate notice and opportunity to be heard and shall remain subject to applicable constitutional limitations.

(22) Independent enforceability of consent. The absence of required voter authorization is an independently enforceable statutory violation, whether or not the particular surveillance practice also violates constitutional search-and-seizure protections.

(23) Enforcement of voter decisions. Upon a finding that an agency is operating without the authorization required by this act, a court shall order cessation of the unauthorized system, consistent with applicable judicial procedure and preservation obligations, and may require independently verified technical shutdown.

(24) No official enforcement veto. Refusal by a government enforcement official to bring an action, or an agency's conclusion that the surveillance technology is operationally useful, shall not by itself supply voter authorization or bar the independent private remedies provided in subsections (14) through (16).

(25) Application of existing sanctions. The vendor penalties, individual civil penalties, victim remedies, audits, and other enforcement mechanisms in this section shall remain applicable to knowing or willful violations of voter-authorization requirements according to their respective elements and culpability standards.

(26) Biometric and association misuse. Knowing or willful violations of the restrictions on generalized biometric identification, unauthorized association mapping, false verification records, or concealed capabilities under Sections 9, 10, 12, and 14 are subject to the otherwise applicable civil penalties, individual remedies, and enforcement procedures of this section according to their respective elements and culpability standards.

Section 17. Judicial Prohibitions and Reinstatement

(1) An enforceable court order prohibiting operation shall take precedence over voter authorization.

(2) A judicial prohibition shall suspend operation but shall not cancel valid authorization, accelerate renewal, or extend its expiration.

(3) If the prohibition ends while authorization remains valid, lawful operation may resume without another election.

(4) If authorization expires while operation is prohibited, voter approval must be obtained again before operation resumes.

(5) A judicial reversal shall not reinstate a system that has never obtained voter approval or whose transitional authority has expired.

(6) No judicial reversal or administrative event shall require or authorize a special election.

(7) Initial authorization obligations may be deferred while a controlling judicial order prohibits operation, but operation may not resume without valid approval where approval is otherwise required.

Section 18. Public Records and Confidentiality

(1) Individually identifying surveillance observations shall not be subject to general public disclosure, except as required by controlling law.

(2) Contracts, expenditures, approved territories, agency policies, aggregate usage statistics, anonymized audit results, enforcement findings, and compliance certifications shall remain publicly accessible.

(3) Public disclosure shall not unnecessarily reveal identifying records of persons incidentally captured.

(4) Lawful discovery, criminal defense rights, judicial process, and legally required evidentiary disclosures shall remain available.

(5) Confidentiality shall not be invoked solely to conceal unlawful surveillance, misuse findings, or material compliance failures.

Section 19. Conforming Amendments

The Legislature shall enact necessary conforming provisions governing:

(1) Election procedures and local ballot authorization;

(2) Municipal and county election administration;

(3) Law enforcement media-record retention;

(4) Public-records confidentiality and judicial access;

(5) Automated license-plate-reader regulations;

(6) Individual statutory liability and governmental indemnification;

(7) Judicial enforcement and assessment of civil penalties; and

(8) Contracting authority and compliance obligations.

Section 20. Construction and Severability

(1) Voter authorization does not establish that a surveillance practice is constitutional.

(2) Nothing in this act shall expand governmental authority to conduct searches, arrests, or surveillance beyond existing constitutional or statutory limits.

(3) Exemptions shall be interpreted according to actual function rather than equipment labels, vendor descriptions, mounting arrangements, or administrative classification.

(4) The act shall govern Idaho state and local operations to the extent permitted by law and shall not purport to bind independent federal or tribal operations beyond the state's lawful authority.

(5) If any provision is found invalid, remaining provisions shall continue to operate to the extent legally and functionally independent.