NxtAssets

Built for Texas

How Purpose-Built Election Asset Management
Meets the Requirements of the Texas Election Code,
EAC Best Practices, and CISA Guidance

Next Election Services, LLC
Austin, Texas
(855) 728-6398 | nxtelection.com
April 2026

Executive Summary

Texas election administrators manage thousands of assets across dozens or hundreds of locations under a regulatory framework that demands strict chain of custody, tamper-evident seal management, continuous tracking, and immutable records. The Texas Election Code (Chapters 66, 125, 127, and 129), Texas Secretary of State advisories, EAC Best Practices, and CISA chain-of-custody guidance all impose specific, overlapping obligations on how voting equipment and election materials are handled, stored, transported, and documented.

Most counties fulfill these obligations with spreadsheets, paper seal logs, and manual processes. That approach works—until it doesn't. A misplaced voting machine, an undocumented seal break, or a gap in the custody record can trigger an audit finding, a public confidence issue, or worse.

NxtAssets by Next Election Services was designed from the ground up to address these Texas-specific requirements. It is not a generic inventory system adapted for elections. It is an election-grade operations platform that embeds Texas Election Code compliance into every workflow, custody event, seal record, and audit log. This white paper maps each regulatory mandate to the NxtAssets capability that addresses it, so that election administrators, Secretary of State staff, and county decision-makers can see exactly how the platform meets the obligations Texas law imposes.

The Texas Regulatory Landscape

Texas county election offices operate under a layered compliance framework. At the state level, the Texas Election Code (TEC) establishes detailed requirements for equipment inventory, chain of custody, transport security, seal management, polling place procedures, and records retention. The Texas Secretary of State issues advisories that provide further operational guidance, particularly around secure storage, seal checks during voting, and recovery plans for custody breaches. At the federal level, the Election Assistance Commission (EAC) publishes best practices for chain of custody and physical security of election equipment, and the Cybersecurity and Infrastructure Security Agency (CISA) provides a chain-of-custody framework for critical infrastructure that election systems fall under.

These requirements are not abstract. They define specific actions: two-person custody transfers, serialized seal logs, secure storage with monitored access, recovery plans with mandatory Secretary of State notification, equipment tracking from storage through coding to deployment and post-election disposition, and records retention for at least 22 months. Failure to demonstrate compliance can result in audit findings, legal exposure, and erosion of public trust.

The sections that follow address each compliance domain in turn, citing the specific statutory provision and showing how NxtAssets meets the requirement.

Pre-Election Security and Inventory

Chapter 129 of the Texas Election Code places detailed obligations on the general custodian of election records regarding the inventory, tracking, storage, and security of electronic information storage media and voting system equipment. These requirements establish the foundation for election security before a single ballot is cast.

Equipment Inventory and Tracking

TEC §129.051(a) requires the general custodian to create and maintain an inventory of all electronic information storage media. **TEC §129.051(b)** requires a procedure for tracking the custody of each storage medium from its storage location, through election coding and the election process, to its post-election disposition and return to storage—with two or more individuals required at each custody transfer.

NxtAssets maintains a central asset registry that supports multiple identifier types per asset: manufacturer serial number, county barcode, RFID tag, Bluetooth BLE tracking beacon, and GPS tracker. Asset Types allow flexible classification with custom attributes, and the registry scales to handle 50,000 or more assets. The platform runs on Oracle 23ai Autonomous Database.

For custody tracking, every handoff event captures both parties' names and IDs, digital signatures collected on a mobile device, timestamp, GPS location, device and network metadata, and event type. These records are stored in Oracle immutable (blockchain) tables—they cannot be altered or deleted, even by a database administrator. Configurable workflows model the full lifecycle from storage through coding, deployment, return, and post-election disposition. Dual-signature enforcement ensures two or more individuals are involved at every custody transfer, as the statute requires.

Secure Storage and Monitoring

TEC §129.051(c) requires a secured location for storing electronic storage media at each phase: when not in use, during coding, during transfer and installation into equipment, and after election parameters are loaded. **TEC §129.051(d)** further requires that coded media remain in the presence of an election official or in a secured location.

NxtAssets tracks asset locations in real time via GPS, BLE, and RFID. Within the warehouse, a mesh of BLE beacons and WiFi access points pinpoints assets to the shelf or station level. Geo-fence boundaries trigger alerts on unauthorized departures. Workflow states such as "In Secure Storage," "In Coding," and "Parameters Loaded" enforce proper transitions. BLE beacon presence detection confirms whether coded media remain within designated secure zones, and GPS trackers on configurable sync intervals (active: 30 seconds, idle: 1 hour) monitor assets at rest. Any departure from a secure zone triggers a real-time alert to designated personnel.

Recovery Plans and Background Checks

TEC §129.051(f) requires a recovery plan for security breaches, including immediate notification to the Secretary of State. **TEC §129.051(g)** requires criminal background checks for relevant election officials, staff, and temporary workers.

NxtAssets provides the detection and documentation layers that support a recovery plan: geo-fence deviation alerts, unexpected seal-break events, and asset separation alerts provide immediate detection of potential breaches. The immutable audit trail provides forensic-quality evidence for investigation. Custom incident-response workflows can be configured to include Secretary of State notification as a mandatory step. Background checks are an HR process external to NxtAssets, but the system enforces the outcome: only provisioned users access the platform. Role-based and attribute-based access controls (RBAC/ABAC) via Oracle APEX and OCI IAM restrict operations by role, and all user actions are audit-logged with user identity, timestamp, and device metadata.

Compliance Summary: TEC §129.051

Citation	What Texas Requires	How NxtAssets Addresses It
§129.051(a)	Maintain inventory of all electronic information storage media.	Central asset registry with multiple identifier types per asset. Scales to 500K+ assets on Oracle 23ai.
§129.051(b)	Track custody from storage through coding, election, and return. Two or more individuals at each transfer.	Chain-of-custody module with dual-signature capture, GPS, timestamps, and immutable blockchain logging. Full lifecycle workflows.
§129.051(c)	Secured location for storage media at each phase.	Real-time location tracking via GPS/BLE/RFID. Geo-fencing with alerts. Workflow-enforced state transitions.
§129.051(d)	Coded media must remain with an official or in secure storage.	Tracker presence detection in secure zones. GPS monitoring at rest. Departure alerts.
§129.051(f)	Recovery plan for breaches; immediate SOS notification.	Real-time alerting, immutable audit trail, configurable incident workflows with SOS notification step.
§129.051(g)	Background checks for election staff.	RBAC/ABAC enforcement. Only provisioned users access the system. All actions audit-logged.

Transport and Custody of Equipment

TEC §129.052 extends the custody and security framework to the transport of voting system equipment. It requires procedures for secure storage and transport (including overnight storage at polling locations), dual-individual custody transfers, a recovery plan for transport security breaches with immediate SOS notification, and a training plan for all relevant personnel.

Transport Lifecycle Management

NxtAssets models the complete transport lifecycle through Work Orders: warehouse loading, delivery, polling-site overnight storage, and return. GPS trackers on vehicles provide continuous in-transit visibility. Dual digital signatures are enforced at every custody transfer. Geo-fences validate correct delivery destinations, and Work Order status tracks actual versus planned handling to identify discrepancies—for example, equipment dropped at the wrong location.

Transport Security Breach Detection

Real-time alerts fire when a vehicle strays from its planned route, an asset departs a geo-fenced location unexpectedly, or a tracked asset separates from its Work Order group. Configurable incident workflows can include Secretary of State notification as a required step, with the event documented in the immutable audit trail.

Staff Training Support

TEC §129.052(c) requires a training plan addressing transport security procedures. NxtAssets workflows function as embedded standard operating procedures—the system guides users through required steps and prevents skipped actions (or at least documents them). Next Election Services provides formal instructor-led training.

Compliance Summary: TEC §129.052

Citation	What Texas Requires	How NxtAssets Addresses It
§129.052(a)	Secure storage and transport procedures, including overnight at polling locations. Dual-individual custody transfers.	Work Orders with delivery workflows, GPS tracking, geo-fence validation, dual-signature chain of custody.
§129.052(b)	Recovery plan for transport breaches; immediate SOS notification.	Geo-fence deviation alerts, asset separation alerts, configurable incident workflows with SOS notification.
§129.052(c)	Training plan for election staff on transport security.	Workflow-embedded SOPs. Formal multi-tier training program with refresher sessions.

Access Control for Voting Equipment

TEC §129.053 requires that access control keys and passwords for voting system equipment be secured, that use be witnessed and documented in a dedicated log, and that the log be retained until the equipment is disposed of.

NxtAssets provides role-based and attribute-based access controls via Oracle APEX and OCI IAM. Every user action is logged with identity, timestamp, device, and network metadata in configurable mutable or immutable logs. Immutable tables have definable retention policies to ensure logs persist through the equipment lifecycle.

Seal Management

Tamper-evident seals are a cornerstone of Texas election security. Multiple sections of the Texas Election Code impose specific obligations on how seals are applied, tracked, and inspected.

Logic and Accuracy Testing Seals

TEC §129.024(a) requires that on completing each test, test materials be placed in a sealed container, with the custodian and at least two testing board members signing the seal. **TEC §129.024(b)–(c)** require that test materials remain sealed for the preservation period, may not be unsealed except for authorized proceedings, and must be resealed when not in use.

NxtAssets tracks every seal by unique serial number and type (tamper-evident, plastic, padlock, etc.). Logic and Accuracy testing workflows include mandatory seal-application steps that cannot be bypassed. The system records which seal ID goes on which container, who applied it, and when. Multi-party chain-of-custody signatures capture the dual-plus witness requirement. Every seal event—application, inspection, removal, reapplication—is logged in the immutable audit trail with timestamp and operator identity. System tracks seal status (intact, broken, replaced) and flags unauthorized unsealing. Oracle immutable tables support definable retention policies aligned with statutory preservation periods (22 months per TEC §129.024(b)).

Ballot Box Seals

TEC §127.064 requires that seals for ballot boxes be serially numbered. **TEC §§127.065–.066** require sealing ballot boxes before delivery to polling places, sealing the deposit slot at close of voting, and delivering sealed ballot boxes to the Central Counting Station.

NxtAssets maintains a serialized seal registry by type, serial number, and current association. Barcode scanning of seal serial numbers ensures accurate association with the correct ballot box or asset. Election workflows include mandatory seal-application steps at each statutory checkpoint: before delivery, at poll close, and before transport to the Central Counting Station. The workflow will not advance to the next state until the seal step is completed and logged. Seal status is visible in real-time dashboards, and the system knows the required sealing points on each asset type.

Compliance Summary: Seal Management

Citation	What Texas Requires	How NxtAssets Addresses It
§129.024(a)	Seal test materials; custodian and two board members sign.	Seal tracking module with workflow-enforced seal steps and multi-party sign-off.
§129.024(b)–(c)	Test materials remain sealed for preservation period; reseal when not in use.	Immutable seal event log. Seal status tracking. Configurable retention policies (22-month minimum).
§127.064	Ballot box seals must be serially numbered.	Serialized seal registry with barcode scanning.
§§127.065–.066	Seal ballot boxes before delivery, at poll close, and before CCS transport.	Workflow-enforced seal checkpoints at each statutory phase.

Equipment Preparation, Delivery, and Installation

TEC §§125.002–.004 require equipment preparation before delivery, Secretary of State–prescribed delivery procedures to prevent tampering and damage, and installation procedures to protect equipment at polling places.

NxtAssets drives equipment preparation through Work Orders with checklists (diagnostic test, firmware update, seal application) and a Product Configurator that generates context-specific Bills of Materials per location type: standard, ADA-enhanced, high-capacity, or early voting. Delivery workflows track loading, transit, and handoff. Setup workflows at polling locations include inspection checklists that must be completed before opening.

Polling Place Security and Closeout

TEC §125.005 requires the presiding judge to periodically inspect voting system equipment for tampering and damage during voting. **TEC §125.063** requires an election officer to secure or inactivate equipment at close of voting to prevent unauthorized operation. **TEC §125.064** requires that documents and records used in or generated by the electronic voting system be available for public inspection during the retention period.

NxtAssets supports routine seal audits on any mobile device via web browser. A poll worker or roving technician can pull up the asset, view expected seals by serial number and seal point, inspect the physical seals, and log an audit pass or fail with a timestamp. Failed audits trigger immediate alerts to administrators, and complete seal audit history is maintained per asset.

The platform provides a Close Poll workflow enforcing all required closeout steps in sequence: seal application, equipment lockdown, packing, and custody transfer recording. Status transitions from “In Use at Polling Location” to “Closed Out” require completion of all checklist items.

For public inspection requirements, NxtAssets provides predefined customizable reports exportable as CSV, document-formatted reports via Word templates, and a natural language query tool for ad-hoc reporting. Immutable tables with configurable retention policies ensure records persist for the required period.

Precinct Records and Retention

TEC §66.021 requires assembling and sealing precinct records in specified envelopes and locked boxes. **TEC §66.058** requires preserving precinct records for 22 months, with voted ballots in a locked room and locked box, and electronic records from Chapter 129 in a secure container. **TEC §66.062** requires following directions on storage and return of boxes, keys, booths, and other equipment.

NxtAssets supports hierarchical multi-level asset nesting—items inside containers inside larger containers. Seal application on record containers is tracked with serial number, timestamp, and operator. Nesting history is maintained so the system knows which items were in which containers at any point.

Oracle immutable tables support definable retention policies set to the statutory 22-month minimum. Physical asset location is tracked continuously via BLE and GPS, and the system detects if a sealed container leaves designated secure storage. Access control logs document who accessed which container and when.

NxtAssets tracks returns via Work Orders and automated location detection. Rally point check-in workflows compare returned assets against expected manifests. Reconciliation reports identify missing, extra, or damaged items, and highlight discrepancies between planned and actual returns.

Central Counting Station Program and Equipment Identification

TEC §§127.123, 127.154–.155 require protecting the tabulation program, assigning permanent identification to tabulators and parts, recording identification on ballot-and-seal certificates, and requiring the presiding judge to sign tabulation tapes.

NxtAssets assigns permanent identifiers to every asset—tabulators, parts, and peripherals—via the multi-identifier registry. Chain-of-custody events with digital signature capture support tabulation tape sign-offs. Seal records link specific seal IDs to specific tabulators for ballot-and-seal certificate data.

Texas Secretary of State Advisory Compliance

Texas SOS Advisory 2019-23 provides operational guidance that supplements the Election Code. Key provisions address seal management during storage, periodic seal checks during voting, and recovery plan requirements.

Secure Storage Seals and Dual-Party Transfers

SOS Advisory 2019-23 §9 requires secure storage to employ uniquely identified tamper-resistant or tamper-evident seals and logs, creation and maintenance of a seal inventory per storage location per election, and two or more individuals at every custody transfer or when equipment has been left unattended.

NxtAssets provides a complete seal registry by type, serial number, and current association (asset, seal point, location). Per-election seal inventory is available via reports. Dual-party custody is enforced at every transfer. BLE and GPS detect when equipment has been unattended outside designated zones.

Seal Checks During Voting

The SOS Advisory (referencing TEC §125.005) requires election officials to periodically check for evidence of tampering on voting equipment during the election. NxtAssets' mobile seal audit interface allows poll workers or roving technicians to scan an asset, view expected seals by serial number and seal point, inspect physical seals, and log pass or fail. Failed audits surface in dashboards and trigger alerts.

Recovery Plan for Seal Damage and Custody Errors

The SOS Advisory requires a written recovery plan for inadvertent seal damage and custody documentation errors, with multi-person confirmation. NxtAssets enforces dual-signature requirements, logs seal damage events with cause codes verified by a second party, immutably records incident events, and produces exportable audit reports for public transparency, FOIA, and observer review.

Federal Alignment: EAC and CISA

EAC Best Practices: Chain of Custody

The Election Assistance Commission's 2021 Best Practices for Chain of Custody recommend at least two signatures on each custody transfer, with the record capturing a detailed description of the item, seal numbers, party names, date and time, location, and signatures. The EAC also recommends that chain-of-custody procedures be available for public inspection before every election and reviewed after each election.

NxtAssets custody events capture all EAC-recommended data points: both parties' names and IDs, digital signatures, timestamp, GPS location, event type and reason, and notes including seal numbers. The dual-party requirement is enforced by workflow—the event is not logged until both signatures are captured. Workflow definitions are stored in JSON, mappable to BPMN, and can be exported, documented, and made available for public inspection. The configurable engine allows post-election review and updates without coding.

EAC Best Practices: Physical Security

The EAC's physical security best practices require safeguards in storage, transit, at the polling place, during voting, and through post-election. These include chain of custody, tamper-evident seals, limiting access, two-person accountability, and access logging.

NxtAssets provides continuous tracking from the warehouse through every phase to post-election. Tamper-evident seals are tracked with serial numbers. All user actions are logged immutably. Dual-signature custody is enforced. GPS and BLE monitoring covers storage and transit. RBAC limits access.

CISA Chain-of-Custody Framework

CISA's 2021 Insights document on Chain of Custody and Critical Infrastructure Systems maps to the NIST Cybersecurity Framework's five functions: Identify, Protect, Detect, Respond, and Recover. NxtAssets addresses each:

Citation	What Texas Requires	How NxtAssets Addresses It
Identify	Inventory all systems, devices, software, data, and people. Document logs. Assess logs for gaps.	Complete asset inventory with multiple identifiers. All transactions logged. Reconciliation reports surface gaps.
Protect	Physical and electronic access control. Continuous monitoring. Manage records for CIA.	RBAC/ABAC via APEX and OCI IAM. TLS in transit, TDE at rest. Immutable blockchain tables. Continuous GPS/BLE monitoring.
Detect	Identify chain-of-custody breaches. Detective measures for anomalies.	Geo-fence alerts, seal-break handling, dashboard anomaly visibility, Work Order discrepancy detection.
Respond	Execute response processes. Document incidents. Review hardware for modification.	Immutable audit trail for forensic-quality incident documentation. Configurable response workflows. Seal audit for modifications.

Recover	Restore from validated versions. Recertification of affected systems.	Asset status tracking. Equipment swap workflows. Quarantine status. Full history export for recertification.

Platform Architecture and Security

NxtAssets runs on Oracle 23ai Autonomous Database on Oracle Cloud Infrastructure (OCI). The platform's architecture provides several layers of security and reliability relevant to county decision-makers:

Immutable Records

Chain-of-custody events, seal records, and critical audit logs are stored in Oracle blockchain tables. These are insert-only, cryptographically chained tables that prevent alteration or deletion—even by a database administrator. The hashing algorithm is SHA2-512. This technology is not an overlay; it is a native feature of the Oracle 23ai database engine.

Encryption

All data at rest is encrypted with AES-256 Transparent Data Encryption (TDE), which is always on in Oracle 23ai Autonomous Database and cannot be disabled. All data in transit is encrypted with TLS 1.2 or 1.3.

Access Control

NxtAssets uses role-based and attribute-based access controls implemented through Oracle APEX and OCI Identity and Access Management. Users are provisioned with specific roles that determine what data they can view and what actions they can perform. Unified auditing—always on in Oracle 23ai—captures all database-level access events.

Availability

The proposed SLA for NxtAssets is 99.995% uptime, backed by Oracle's Autonomous Database infrastructure with automated patching, scaling, and failover.

Cloud Infrastructure

OCI commercial regions are the default deployment, with OCI Government Cloud (FedRAMP High) available on demand for counties that require it.

About Next Election Services

Next Election Services, LLC (NES) is an Austin-based company founded in 2025 by a team of senior election technology professionals with decades of combined experience serving Texas counties and election offices nationwide. The NES team has deep operational knowledge of Texas election administration, the Texas Election Code, and the specific challenges county election offices face.

NxtAssets is the company's flagship product—an election-grade asset management platform designed specifically for the unique demands of elections. NES also offers NxtPortal, a voter communication and ballot tracking product.

See NxtAssets in Action

To schedule a demo, discuss your county's specific requirements, or request a copy of the full NxtAssets Compliance Crosswalk, contact Next Election Services:

Next Election Services, LLC

Phone: (855) 728-6398

Web: nxtelection.com

Email: info@nxtelection.com